EL DELITO INFORMATICO EN LA LEGISLACION COLOMBIANA

SANTIAGO BARRIOS SOLANO

CORPORACIÓN UNIVERSITARIA DE LA COSTA C.U.C.
PROGRAMA DE DERECHO
BARRANQUILLA
2012

EL DELITO INFORMATICO EN LA LEGISLACION COLOMBIANA

SANTIAGO BARRIOS SOLANO

Trabajo de Grado presentado como requisito para optar al título de ABOGADO

ALAIT FREJA CALAO
Asesor del Proyecto

CORPORACIÓN UNIVERSITARIA DE LA COSTA C.U.C.
PROGRAMA DE DERECHO
BARRANQUILLA
2012

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

PRESIDENTE DEL JURADO

_____

JURADO

Barranquilla, Febrero de 2012

AGRADECIMIENTOS

A Dios, por permitir que a pesar de las dificultades terminara mis estudios universitarios y siempre ha estado presente en cada pequeño logro que he alcanzado a lo largo de mi vida.

A mi papá que con su esfuerzo y dedicación logró cultivar en mí una persona llena de principios, con ganas de seguir adelante y en especial, capaz de construir su futuro. Q.E.P.D.

A mis familiares, especialmente a Wilson Enrique Barrios Serje porque estuvo apoyándome en el diseño de esta investigación y me colaboró en todo lo que necesité en el proceso. Q.E.P.D.

A todas esas personas anónimas que sin saberlo hicieron parte de mi formación y de la realización de este proyecto.

DEDICATORIA

Este trabajo de grado se la dedico primero a Dios, quien me ha dado las fuerzas, inteligencia, conocimiento y sabiduría para alcanzar mis objetivos y seguir caminando para llegar a la meta.

A mi madre que siempre me ha brindado su amor puro y su apoyo incondicional cuando más lo he necesitado.

A mi tío que siempre creyó en mí.

A mis familiares que me llenan de motivos para pensar en un mejor mañana.

A mi Universidad que sin pensarlo se convirtió en un segundo hogar capaz de brindarme conocimiento y a su vez mucho cariño utilizando como instrumento a sus docentes.

Gracias.

Santiago Andrés Barrios Solano

EL DELITO INFORMATICO EN LA LEGISLACION COLOMBIANA

PALABRAS CLAVES

BOMBA LOGICA: Es una parte de un código informático insertada intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones preprogramadas, en ese momento se ejecuta una acción maliciosa que puede ocasionar daños irreparables al sistema general de la computadora.

CABALLO DE TROYA O TROYANO: En la informática se denomina troyano o caballo de Troya a un software maligno que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños. El término troyano proviene de la historia del caballo de Troya mencionado en la Odisea de Homero.

CRIMINALIDAD: El termino criminalidad, que a su vez procede del latín criminalis, significa tanto la calidad o circunstancia que hace que una acción sea delictiva, como el cómputo de los crímenes o delitos cometidos en un territorio y tiempo determinado. Luis Bohórquez Botero jurista e investigador colombiano, coautor del diccionario jurídico nacional la define como “la correlación existente

entre la contextura general de la sociedad y la cuantía y la calidad de la delincuencia, es un hecho ya constatado por la ciencia"[1].

GLOBALIZACION: Es un proceso económico, tecnológico, social y cultural a gran escala, que consiste en la creciente comunicación e interdependencia entre los distintos países del mundo unificando sus mercados, sociedades y culturas, a través de una serie de transformaciones sociales, económicas y políticas que les dan un carácter global. La globalización es a menudo identificada como un proceso dinámico producido principalmente por las sociedades que viven bajo el capitalismo democrático o la democracia liberal y que han abierto sus puertas a la revolución informática, plegando a un nivel considerable de liberalización y democratización en su cultura política, en su ordenamiento jurídico y económico nacional, y en sus relaciones internacionales.

HARDWARE: Corresponde a todas las partes físicas y tangibles de una computadora; sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado; contrariamente, el soporte lógico es intangible, y que es llamado software. El término es propio del idioma ingles (literalmente

[1] BOHORQUEZ BOTERO, Luis Fernando. Diccionario Jurídico Colombiano. Séptima Edición. Ed. Jurídica Nacional, 2006. Pág. 562

traducido: partes duras), su traducción al español no tiene un significado acorde, por tal motivo se la ha adoptado tal cual es y suena; la Real Academia Española lo define como “Conjunto de los componentes que integran la parte material de una computadora”.

INFORMATICA: Disciplina que se ocupa del tratamiento racional de la información, utilizando para ello los impresionantes y acelerados avances que en materia de computación y ciencias tecnologías sucede en nuestros tiempos.

INTERNET: Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos. Uno de los servicios que más éxito ha tenido en Internet ha sido la World Wide Web (WWW, o "la Web"), hasta tal punto que es habitual la confusión entre ambos términos. La WWW es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de hipertexto. Ésta fue un desarrollo posterior (1990) y utiliza Internet como medio de transmisión. Existen, por tanto, muchos otros servicios y protocolos en Internet, aparte de la Web: el envío de correo electrónico (SMTP), la transmisión de archivos (FTP y P2P), las conversaciones

en línea (IRC), la mensajería instantánea y presencia, la transmisión de contenido y comunicación multimedia telefonía (VoIP), televisión (IPTV), los boletines electrónicos (NNTP), el acceso remoto a otros dispositivos (SSH y Telnet) o los juegos en línea.

REDES SOCIALES: son estructuras sociales compuestas de grupos de personas, las cuales están conectadas por uno o varios tipos de relaciones, tales como amistad, parentesco, intereses comunes o que comparten conocimientos.

En su forma más simple, una red social es un mapa de todos los lazos relevantes entre todos los nodos estudiados. Se habla en este caso de redes "sociocéntricas" o "completas". Otra opción es identificar la red que envuelve a una persona (en los diferentes contextos sociales en los que interactúa); en este caso se habla de "red personal".

REVOLUCION INFORMATICA: Este fue el nombre que se le otorgó al fenómeno que revolucionó al mundo, debido a su impacto social por la cantidad de personas involucradas directa o indirectamente en actividades relacionadas con el uso de la informática. Sin embargo, aún cuando el número de personas que se encuentran directamente empleadas en actividades informáticas es relativamente pequeño respecto al total de la fuerza de trabajo, si consideramos

actividades que indirectamente dependen de la informática, como las actividades bancarias y de seguros, de los gobiernos centrales y locales, así como educación y entrenamiento, es claro que un buen porcentaje de la fuerza de trabajo gira alrededor de la informática. Y dado que todos utilizamos información en algún momento, eventualmente no habrá nadie que no sea afectado por la Revolución Informática, ya que finalmente, información es el flujo vital de las sociedades industriales modernas.

SOFTWARE: Esto hace referencia al equipamiento lógico o soporte lógico de una computadora digital; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos, que son llamados hardware.

Los componentes lógicos incluyen, entre muchos otros, las aplicaciones informáticas; tales como el procesador de textos, que permite al usuario realizar todas las tareas concernientes a la edición de textos; el software de sistema, tal como el sistema operativo, que, básicamente, permite al resto de los programas funcionar adecuadamente, facilitando también la interacción entre los componentes físicos y el resto de las aplicaciones, y proporcionando una interfaz para el usuario.

TERRORISMO: Este fenómeno del terrorismo es el uso sistemático del terror, para coaccionar a sociedades o gobiernos, utilizado por una amplia gama de organizaciones políticas en la promoción de sus objetivos, tanto por partidos políticos nacionalistas y no nacionalistas, de derecha como de izquierda, así como también por grupos religiosos, racistas, colonialistas, independentistas, revolucionarios, conservadores, ecologistas y gobiernos en el poder.

VIRUS INFORMATICO: Es un programa dañino también conocido como Malware, este tiene por objeto alterar el normal funcionamiento de la computadora sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

RESUMEN

Para abarcar el tema de la delincuencia informática cabe resaltar que este tópico se originó con el auge del internet en el mundo a mediados de los noventa y así fue aumentando proporcionalmente con su desarrollo en el ámbito internacional. Se debe entender como delito informático toda acción u omisión realizada por un ser humano mediante un medio tecnológico que cause daño a personas sin que su autor se obtenga un beneficio propio o para terceros.

En esta especialidad de delito intervienen el sujeto activo, el cual posee características particulares como lo son los conocimientos elevados acerca del funcionamiento de la informática y de cuáles eran sus debilidades, mientras que el sujeto pasivo es indeterminado, debido a que cualquier esfera social es susceptible a este nuevo y complejo flagelo.

En Colombia se tipificaron estas conductas punibles con entrada en vigencia de la Ley 1273 de 2009, después de una prolongada y lenta evolución legislativa, que adoptó experiencias internacionales de países en donde ya venían enfrentando esta problemática. Dicha ley brindó un marco jurídico sostenible en el cual se permitiera sancionar con severidad y efectividad la delincuencia informática además de reducir los índices de impunidad que se registraban por la atipicidad de muchas conductas realizadas a través de medios tecnológicos.

COMPUTER CRIME LEGISLATION IN COLOMBIA

KEYWORDS

LOGIC BOMB: A portion of computer code intentionally inserted into a computer program that remains hidden until conditions met one or more presets, and then run malicious actions that can cause irreparable damage to the overall computer system.

TROJAN HORSES OR TROJAN: In computer called Trojan or a Trojan horse malware that the user is presented as a seemingly legitimate program and harmless but when run causes damage. The term Trojan comes from the history of the Trojan horse mentioned in Homer's Odyssey.

CRIME: The term crime, which in turn comes from the Latin criminalis, means either the quality or circumstance that makes an action is criminal, as the computation of the crimes or offenses committed in a territory and time. Luis Bohorquez Botero jurist Colombian researcher, author of the national legal dictionary defines it as "the correlation between the general texture of society and the amount and quality of crime is a fact already confirmed by science."

GLOBALIZATION: It is an economic, technological, social and cultural scale, which consists of increasing communication and interdependence among countries in the world by unifying its markets, societies and cultures, through a series of social, economic and political those give a global character.

Globalization is often identified as a dynamic process mainly produced by societies living under democratic capitalism or liberal democracy and who have opened their doors to the information revolution, folding to a considerable degree of liberalization and democratization of its political culture, in its legal system and national economic and international relations.

HARDWARE: Applies to all physical and tangible parts of a computer, electrical components, electronic, electromechanical and mechanical, its cables, cabinets or boxes, peripherals of all kinds and any other physical element involved; contrary, software is intangible, and is called software. The term is characteristic of the English language (literally translated: hard parts), a Spanish translation does not have a consistent meaning for that reason it has been adopted as it is and sounds, the Spanish Royal Academy defines it as "A set of components that make up the material part of a computer. "

COMPUTER: Discipline that deals with the rational treatment of information, using the impressive and rapid advances in computer technology and science going on in our time.

INTERNET: A set of decentralized communications networks interconnected using the family of TCP / IP, ensuring that the heterogeneous physical networks that compose it work as a single logical network, worldwide. Its origins date back to 1969, when he established the first connection of computers, known as

ARPANET, between three universities in California and one in Utah, USA. One of the services most successful on the Internet has been the World Wide Web (WWW or "Web"), to the point that is common confusion between the two. The WWW is a set of protocols that allows a simple, remote consultation hypertext files. This was a later development (1990) and uses the Internet as the transmission medium. There are, therefore, many other Internet services and protocols besides the Web: sending email (SMTP), file transfer (FTP and P2P), online conversations (IRC), instant messaging and presence the transmission of multimedia content and communication telephony (VoIP), television (IPTV), electronic newsletters (NNTP), remote access to other devices (SSH and Telnet) or online games.

SOCIAL NETWORKS: are social structures composed of groups of people, which are connected by one or more types of relationships such as friendship, kinship, common interests or shared knowledge.

In its simplest form, a social network is a map of all the relevant links between all nodes studied. We speak here of networks "sociocentric" or "complete". Another option is to identify the network that involves a person (in different social contexts in which they interact), in which case we speak of "personal network".

COMPUTER REVOLUTION: This was the name that was given to the phenomenon that revolutionized the world because of its social impact by the number of people involved directly or indirectly in activities related to the use of information technology. However, even if the number of people who are directly engaged in computer activities is relatively small compared to the total workforce, if we consider activities that indirectly depend on the computer, such as banking and insurance, government central and local, and education and training, it is clear that a good percentage of the labor force revolves around the computer. And since we all use information at some point, eventually no one will be unaffected by the Information Revolution, and finally, information is the lifeblood of modern industrial societies.

SOFTWARE: This refers to the logical equipment or software of a digital computer, comprising all the necessary software components that enable specific tasks, as opposed to the physical components, which are called hardware.

The logical components include, among others, computer applications, such as word processor, which allows the user to perform all tasks related to text editing, the system software, such as operating system, which basically allows the rest of the programs function properly, also facilitating the interaction between the

physical components and the rest of the applications, and providing an interface for the user.

TERRORISM: The phenomenon of terrorism is the systematic use of terror, to coerce societies or governments, used by a wide range of political organizations in promoting its objectives, both for nationalist political parties and non-nationalist, right and left, as well as religious groups, racist, colonialist, independence, revolutionary conservatives, environmentalists and governments in power.

COMPUTER VIRUS: A malicious program also known as Malware, this is to alter the normal functioning of the computer without permission or knowledge of the user. The virus usually replaces other executable files infected with this code. Viruses can destroy, intentionally, the data stored on a computer, although other more harmless, which is only characterized by being annoying.

ABSTRAC

To cover the issue of cybercrime is worth noting that this topic originated with the rise of the Internet in the world in the mid-nineties and it was increasing in proportion to its development internationally. It should be understood as computer crime any act or omission by a human being through a technological medium that causes harm to people without the author to obtain a benefit or for others.

This specialty of offense involved the offender, which has particular characteristics such as high knowledge about the workings of the computer and what their weaknesses, while the victim is unknown, because any social sphere is susceptible this new and complex scourge.

In Colombia, classify this conduct punishable with effective date of Act 1273 of 2009, after a long, slow change in legislation, which adopted international experiences of countries which were already facing this problem. This law provided a legal framework in which sustainable allow severely punish cybercrime and effectiveness while reducing levels of impunity that were recorded by the unusualness of many behaviors made through technological means.

CONTENIDO

Pág.

INTRODUCCIÓN

A lo largo de la historia el hombre ha necesitado transmitir y tratar la información de forma continua. Aun están en el recuerdo las señales de humo y los destellos con espejos, y más recientemente los mensajes transmitidos a través de cables utilizando el código Morse, o la propia voz por medio del teléfono. La humanidad no ha cesado en la creación de métodos para procesar información. Con ése fin nace la informática, como ciencia encargada del estudio y desarrollo de estas máquinas y métodos, y además con la idea de ayudar al hombre en aquellos trabajos rutinarios y repetitivos, generalmente de cálculo o de gestión.

La información al alcance de millones de personas de todo el mundo, delincuentes diversos encontraron el modo de contaminarla y lo que es peor, ataques a la red y que podemos calificar corno de los más graves es el uso de la red por parte de la mafia internacional que maneja la prostitución infantil, por el terrorismo internacional y también por el narcotráfico, no solo en Colombia sino en el mundo, ya que en todo el globo no se ha tipificado el mismo como delito autónomo.

Políticos de algunos países han pedido que se reglamente el uso de la red, de modo que quienes prestan el servicio de Internet registren a los clientes,

cuándo y dónde llaman y para qué, pero la iniciativa hizo que, en defensa de la libertad y de la privacidad, muchos usuarios honestos y algunas empresas que participan de los beneficios económicos de la red, protestaran enérgicamente. El desarrollo de las tecnologías informáticas ofrece un aspecto negativo: Ha abierto la puerta a conductas antisociales y delictivas.

Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas para infringir la ley y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

El objetivo de este trabajo es describir, Las conductas delictivas que pueden generar el gran avance tecnológico, sobre todo en el campo de la informática desde un punto de vista normativo.

La cifra negra de la criminalidad, en materia de delitos informáticos, no puede seguir en la penumbra, de allí la necesidad imperiosa para el derecho penal y organismos gubernamentales la investigación de una nueva modalidad comisiva de amplias repercusiones sociales y económicas. Existe una necesidad urgente de incluir en el derecho penal vigente una tipificación básica de los delitos informáticos que afecten el interés social y el patrimonio público. En primer término en lo que concierne a las conductas punibles, sería

imprescindible crear nuevos tipos penales y en otros casos modificar los ya existentes.

De otra parte, sería importante, resolver el problema de la atipicidad relativa generada por la ausencia de uno de los elementos del tipo cuando se trata de subsumir la conducta ilícita. Las infracciones ostensiblemente antijurídicas que recaen sobre ciertos bienes informáticos como el caso del Software.

Actualmente se requieren serias modificaciones y en otros casos nuevas normas para disminuir en cierta forma la incertidumbre jurídica en que se encuentran sumergidas las nuevas disposiciones penales en materia de delito informático, pese a algunos avances, como te tipificación del acceso abusivo a sistemas informáticos en el nuevo estatuto represor. Cada vez más, se hace necesario el respaldo legal como la mejor y más adecuada forma de reprimir y castigar estos delitos, tal como se expondrá en el capítulo de la conveniencia de su incriminación y el sistema más adecuado para Colombia, según su tradición jurídico - legal. Las conductas reprochables, resultan en la mayoría de los casos impunes debido a la idoneidad de las figuras incriminatorias tradicionales, a no ser castigados dichos comportamientos ilícitos, debido a la carencia de claridad sobre la naturaleza jurídica de los bienes objeto material de los delitos ni del interés jurídico protegido.

Finalmente se expondrán cada uno de los avances en materia normativa de los delitos informáticos en la legislación colombiana, que necesita de verdaderos cambios, con miras de que exista en Colombia una penalización de la criminalidad informática. Al igual que un capítulo de recomendaciones donde se expondrán ideas, sobre la forma como enfrentar esta problemática social.

El estado actual de adecuación normativa está en una categoría sui generis, ya que dichas infracciones no son de recibo en las actuales formas descriptivas, pese a que ya las contienen la mayoría de legislaciones penales.

Crear o modificar es el dilema, estudiar si conviene crear una ley individual sobre la materia o si los diversos tipos penales deben ser encasillados en diferentes capítulos del Código Penal mediante la ampliación de algunos tipos penales, esta es la situación que se va a describir en la investigación.

1. ORIGEN DEL DELITO INFORMÁTICO

1.1 RESEÑA HISTORICA

Sus orígenes se remontan a los años sesenta cuando los Estados Unidos consideraron la necesidad de integrar sus redes de información militar de forma tal que la salida del aire de una de ellas no afectara la comunicación entre las otras y que permitiese a los usuarios autorizados tener acceso a todas ellas al conectarse a una de las redes interconectadas. Aquel pasado bélico corresponde a la llamada ARPANET (Advanced Research Projects Agency Network o Red de la Agencia para los Proyectos de Investigación Avanzada de los Estados Unidos), que nos legó el trazado de una red inicial de comunicaciones de alta velocidad a la cual fueron integrándose otras instituciones gubernamentales y redes académicas durante los años setenta.

Investigadores, científicos, profesores y estudiantes se beneficiaron de la comunicación con otras instituciones y colegas en su rama, así como de la posibilidad de consultar la información disponible en otros centros académicos y de investigación. De igual manera, disfrutaron de la nueva habilidad para publicar y hacer disponible a otros la información generada en sus actividades.
En el mes de Julio de 1961 Leonard Kleinrock publicó desde el MIT (Instituto Tecnológico de Massachusetts) el primer documento sobre la teoría de

conmutación de paquetes. Kleinrock convenció a Lawrence Roberts de la factibilidad teórica de las comunicaciones vía paquetes en lugar de circuitos, lo cual resultó ser un gran avance en el camino hacia el trabajo informático en red. El otro paso fundamental fue hacer dialogar a los ordenadores entre sí. Para explorar este terreno, en 1965, Roberts conectó una computadora TX2 en Massachusetts con un Q-32 en California a través de una línea telefónica conmutada de baja velocidad, creando así la primera (aunque reducida) red de computadoras de área amplia jamás construida.

La primera red interconectada nace el 21 de Noviembre de 1969, cuando se crea el primer enlace entre las universidades de California en los Ángeles y Standford por medio de la línea telefónica conmutada, y gracias a los trabajos y estudios anteriores de varios científicos y organizaciones desde 1959. El mito de que ARPANET, la primera red, se construyó simplemente para sobrevivir a ataques nucleares sigue siendo muy popular. Sin embargo, este no fue el único motivo. Si bien es cierto que ARPANET fue diseñada para sobrevivir a fallos en la red, la verdadera razón para ello era que los modos de conmutación eran poco confiables para un uso exclusivo.

A raíz de un estudio de RAND (Corporación Estadounidense creada para ofrecer investigación y análisis a las fuerzas armadas), se extendió el falso rumor de que ARPANET fue diseñada para resistir un ataque nuclear. Esto

nunca fue cierto, solamente un estudio de RAND, no relacionado con ARPANET, consideraba la guerra nuclear en la transmisión segura de comunicaciones de voz. Sin embargo, trabajos posteriores enfatizaron la robustez y capacidad de supervivencia de grandes porciones de las redes subyacentes. (Internet Society, A Brief History of the Internet).

Posteriormente en 1972 Se realizó la Primera demostración pública de ARPANET, una nueva red de comunicaciones financiada por la DARPA (La Agencia de Investigaciones de Proyectos Avanzados de Defensa) que funcionaba de forma distribuida sobre la red telefónica conmutada. El éxito de ésta nueva arquitectura sirvió para que, en 1973, la DARPA iniciara un programa de investigación sobre posibles técnicas para interconectar redes (orientadas al tráfico de paquetes) de distintas clases. Para este fin, desarrollaron nuevos protocolos de comunicaciones que permitiesen este intercambio de información de forma "transparente" para las computadoras conectadas. De la filosofía del proyecto surgió el nombre de "Internet", que se aplicó al sistema de redes interconectadas mediante los protocolos TCP e IP.

Mas tarde el 1 de Enero de 1983, ARPANET cambió el protocolo NCP (Network Control Program) por TCP/IP. Ese mismo año, se creó el IAB (Comité encargado de la supervisión del desarrollo técnico y de la ingeniería del Internet) con el fin de estandarizar el protocolo TCP/IP y de proporcionar

recursos de investigación a Internet. Por otra parte, se centró la función de asignación de identificadores en la IANA (Internet Assigned Numbers Authority) que, más tarde, delegó parte de sus funciones en el Internet registry que, a su vez, proporciona servicios a los DNS.

Para el año de 1986 la NSF comenzó el desarrollo de NSFNET que se convirtió en la principal Red en árbol de Internet, complementada después con las redes NSINET y ESNET, todas ellas en Estados Unidos. Paralelamente, otras redes troncales en Europa, tanto públicas como comerciales, junto con las americanas formaban el esqueleto básico ("backbone") de Internet.

Luego en 1989 con la integración de los protocolos OSI en la arquitectura de Internet, se inició la tendencia actual de permitir no sólo la interconexión de redes de estructuras dispares, sino también la de facilitar el uso de distintos protocolos de comunicaciones.

En el CERN de Ginebra (Modelo de colaboración científica internacional), un grupo de físicos encabezado por Tim Berners-Lee creó el lenguaje HTML, basado en el SGML. En 1990 el mismo equipo construyó el primer cliente Web, llamado WorldWideWeb (WWW), y el primer servidor web.

A inicios de los 90, con la introducción de nuevas facilidades de interconexión y herramientas gráficas simples para el uso de la red, se inició el auge que actualmente le conocemos al Internet. Este crecimiento masivo trajo consigo el surgimiento de un nuevo perfil de usuarios, en su mayoría de personas comunes no ligadas a los sectores académicos, científicos y gubernamentales.

Esto ponía en cuestionamiento la colaboración del gobierno estadounidense al sostenimiento y la administración de la red, así como la prohibición existente al uso comercial del Internet. Los hechos sucedieron rápidamente y para 1993 ya se había levantado la prohibición al uso comercial del Internet y definido la transición hacia un modelo de administración no gubernamental que permitiese, a su vez, la integración de redes y proveedores de acceso privados.

En consecuencia para el año 2006, exactamente el 3 de enero, Internet había alcanzado los mil cien millones de usuarios y se prevé que en diez años, la cantidad de navegantes de la Red aumentará a dos mil millones, cantidades expuestas por el Washington Post, famoso diario de amplia circulación en Norte América.

En este orden de ideas era evidente que la transformación de lo que fue una enorme red de comunicaciones para uso gubernamental, planificada y construida con fondos estatales, había evolucionado en un sinnúmero de redes

privadas interconectadas entre sí. Que cada día experimenta la integración de nuevas redes y usuarios, extendiendo su amplitud y dominio, al tiempo que surgen nuevos mercados, tecnologías, instituciones y empresas que aprovechan este nuevo medio, cuyo potencial apenas se comienza a descubrirse.

El hecho de que Internet haya aumentado tanto implica una mayor cantidad de relaciones virtuales entre personas del común lo que hace posible concluir que cuando una persona tenga una necesidad de conocimiento no escrito en libros, podría recurrir a una fuente más acorde a su necesidad. Como ahora esta fuente es posible en Internet como toda gran revolución, Internet augura una nueva era de diferentes métodos de resolución de problemas creados a partir de soluciones anteriores.

1.2 CONCEPTUALIZACIÓN DE LOS DELITOS INFORMÁTICOS.

Anteriormente la legislación colombiana carecía de un tipo penal que describiera y penalizara la delincuencia informática, por consiguiente la estafa se convirtió en el tipo penal más utilizado por el operador judicial para poder castigar este nuevo fenómeno delincuencial. La estafa puede ser definida como un engaño, una acción contradictoria a la verdad o a la rectitud, pero la Conceptualización de Delito puede ser mucho más compleja.

Muchos estudiosos y autores del Derecho Penal han intentado formular una noción de delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible dada la íntima conexión que existe entre la vida social y la jurídica de cada pueblo y obviamente aquella condiciona a ésta.

Se podría definir el delito informático como toda acción u omisión culpable realizada por un ser humano mediante un medio tecnológico, que cause un perjuicio a personas sin que necesariamente el autor logre un beneficio propio, o a terceros. En este orden de ideas el autor mexicano Julio Téllez Valdez divide a los delitos informáticos en dos conceptos que son el atípico y el típico señalando que los delitos informáticos "son actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)"[2].

En los últimos años las terminales o computadoras se utilizaron no solo como herramientas que auxiliaron la labor de los humanos y que sirvió de apoyo técnico a los mismos, sino que también fueron un medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación, y condiciona su desarrollo de la informática; tecnología cuya

[2] TELLEZ VALDEZ, Julio. Derecho informático. Tercera Edición. México: Ed. Mc Graw Hill, 1999. Pág. 104.

esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos.

Puede sostenerse entonces que las perspectivas de la informática no tienen límites previsibles y que aumentan en forma que aún puede impresionar a muchos actores del proceso.

Debido a esta vinculación, el aumento del nivel de los delitos relacionados con los sistemas informáticos registrados en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, representa una amenaza para la economía de un país y también para la sociedad en su conjunto.

Actualmente la informatización se ha implantado en todos los países. Tanto en la organización administrativa de las empresas y administraciones públicas como en la investigación científica, en la producción industrial o en el estudio e incluso en actividades de recreación, el uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que presenta comienzan a surgir algunas facetas negativas, como por ejemplo, lo que ya se conoce como crímenes informáticos.

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación

fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos, el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales. Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse jamás.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, etc.). La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

La importancia reciente de los sistemas de datos, por su gran incidencia en la marcha de las empresas, tanto públicas como privadas, los ha transformado en un objeto cuyo ataque provoca un perjuicio enorme, que va mucho más allá del valor material de los objetos destruidos. A ello se une que estos ataques son

relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante allá de alcanzar los objetivos sin ser descubiertos.

Recientemente el departamento de investigación de la Universidad de México ha realizado un importante desarrollo del tema desde el punto de vista normativo del que se transcribe alguna de sus partes. Entienden que "delitos informáticos" son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.

El delito Informático implica actividades criminales que un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como el hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc., sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.

No hay definición de carácter universal propia de delito Informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aun cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas.

Los delitos informáticos, en general, son aquellos actos delictivos realizados con el uso de computadoras o medios electrónicos, cuando tales conductas constituyen el único medio de comisión posible o el considerablemente más efectivo, y los delitos en que se daña estos equipos, redes informáticas, o la información contenida en ellos, vulnerando bienes jurídicos protegidos. Es decir, son los delitos en que los medios tecnológicos o son el método o medio comisivo, o el fin de la conducta delictiva.

El intelectual jurista colombiano Alexander Díaz García afirma que “el delito informático en un sentido más amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin, y que, en un sentido estricto, el delito Informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin"[3].

Por otra parte, se debe mencionar que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa a la computadora, tales como delitos informáticos, delitos electrónicos, delitos relacionados con la computadora, crímenes por computadora, delincuencia relacionada con el ordenador.

[3] DÍAZ GARCÍA, Alexander. Derecho informático. Elementos de la Informática Jurídica. Bogotá: Editorial Leyer, 2007. Pág. 79

1.3 LA TIPICIDAD EN LOS DELITOS INFORMÁTICOS

La tipicidad es un elemento del delito que consiste en la perfecta adecuación en la total conformidad, entre un hecho de la vida real y algún tipo legal, o tipo penal. En este sentido el jurista Luis Fernando Bohórquez Botero, establece que la tipicidad es:

> Una de las principales conquistas del constitucionalismo pues constituye una salvaguarda de la seguridad jurídica de los ciudadanos ya que les permite conocer previamente cuándo y por qué motivos pueden ser objeto de penas ya previstas en el ordenamiento jurídico. De esta manera la tipicidad protege la libertad individual, controla la arbitrariedad judicial y asegura la igualdad de las personas ante el poder punitivo estatal.[4]

En lo que se refiere a la tipificación de los delitos informáticos, la discusión a nivel doctrinario ha sido ardua y controversial. Doctrinarios especialistas en Derecho Penal tanto en el ámbito nacional como internacional se han enfrentado a diversas consideraciones.

Una de ellas, es la referente a establecer cuales conductas censurables podrían ser reglamentadas de mejor manera por otras ramas del Derecho y cuáles de ellas merecen un tratamiento punible.

[4] Op.Cit. BOHORQUEZ BOTERO, Luis Fernando. Pág. 609

Todo esto se observa por la consideración que se le tiene al Derecho penal como última ratio, quiere decir esto entonces, que cuando las normas jurídicas existentes y establecidas por otras ramas del Derecho no sean suficientes para controlar la lesión de bienes jurídicos protegidos y regulados en el ámbito constitucional y supra constitucional, debe acudirse entonces al Derecho Penal como última instancia, debido a que esta es la rama del Derecho que establece las sanciones más fuertes, al imponer penas tales como la privativa de libertad.

Otra de las consideraciones es la referente a decidir si es necesario y conveniente crear una ley individual sobre la materia en estudio, o si los diversos tipos penales informáticos deben ser encasillados en los capítulos ya existentes del Código Penal, obedeciendo claro está, al interés jurídico que con ellos resulte afectado, lo que sin lugar a dudas llevaría a una reforma de nuestro Código Penal y por ende al procedimental.

Si bien se observa que en ciertos casos los tipos penales definidos en el Código Penal pueden ser aplicables a las conductas explicadas en la clasificación de los delitos informáticos, también es cierto que las mismas, resultan insuficientes frente a las nuevas necesidades de la colectividad y la evolución acelerada de la sociedad, y, además, dado que en el Derecho Penal está prohibida la aplicación analógica de los tipos debido al reconocimiento del principio de legalidad; por tal motivo de no generar la creación de nuevas figuras

delictuosas, en nuestra legislación Colombiana, numerosas conducías a pesar de su contenido criminal continuarían quedando sin la aplicación de sanciones penales.

1.4 CONCEPTUALIZACIÓN DEL CÓDIGO PENAL COLOMBIANO

El Código Penal Colombiano expedido con la Ley 599 de 2000, no hacía referencia expresa a los delitos informáticos como tales, no obstante, en varias de sus normas recogía conductas que podrían entenderse incorporadas al concepto que la doctrina había desarrollado sobre el tema. Esto hasta la entrada en vigencia de la ley 1273 del 2009 que tipificó conductas que anteriormente eran inexistentes en el antiguo código, creando nuevos tipos penales relacionados con los delitos informáticos y la protección de la información e introduciendo un nuevo bien jurídico tutelado.

Si se tiene en cuenta el desarrollo doctrinal del tema, se encuentra que el concepto de "delito informático" puede comprender tanto aquellas conductas que recaen sobre herramientas informáticas propiamente, llámense programas, ordenadores, etc., como aquellas que valiéndose de estos medios lesionan otros intereses jurídicamente tutelados como son la intimidad, el patrimonio económico, la fe pública, etc.

Se observa entonces que la diferencia entre la violación ciertos derechos tales como la intimidad o el patrimonio económico serian el medio a través del cual se está cometiendo la conducta, obteniendo el mismo fin.

1.5 CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS

El doctor Julio Téllez Valdez[5] clasifica a los delitos informáticos con base en dos criterios, y que son los acogidos por muchos autores, motivo por el cual se hace la referencia correspondiente, y se hace especial énfasis en su clasificación:

- *Como instrumento o medio*.
- *Como fin u objetivo.*

1.5.1 Como Instrumento o Medio. Esta clasificación se refiere al grupo de conductas que infringen los sistemas que utilizan medios tecnológicos de información, en otras palabras, son conductas que lesionan bienes jurídicos constituidos por la información y datos que los sistemas contienen, procesan, resguardan y transmiten, de manera que la información no es más que el bien que subyace en ellos.

[5] Op. Cit. TELLEZ VALDEZ, Julio. Pág. 204

1.5.2 Como fin u objetivo. Esta segunda clasificación, correspondiente a los delitos informáticos de medio, recopila las conductas que se aprovechan del uso de los medios tecnológicos de información para atentar contra bienes jurídicos distintos a la información que se contiene en los mismos y tratada en sistemas automatizados, esto es, bienes como la propiedad, la privacidad de las personas o el orden económico. Lo que distingue a este grupo de delitos informáticos es el aprovechamiento de las tecnologías de información como el único medio de comisión posible o como medio extremadamente ventajoso en relación con cualquier otro para afectar el bien jurídico que este resguardado o bajo protección del derecho penal.

1.6 SUJETOS DE LA RELACIÓN JURÍDICO DELICTUAL EN MATERIA DE DELITO INFORMÁTICO.

La mayoría de las personas que cometen delitos informáticos ostentan ciertas particularidades o características específicas, tales como la habilidad para el uso y manejo de los sistemas informáticos o la facilidad de ejecución de tareas laborales que pueden facilitarles el acceso a la información de carácter privado.

Generalmente lo que lleva a algunas personas a realizar delitos informáticos, no es tan solo la parte económica, sino que se refiere al deseo de desarrollar y

darle a conocer a otras personas de las habilidades y conocimientos que el delincuente pueda llegar a tener sobre la materia.

1.6.1 Sujeto Activo. La mayoría de los autores sobre delitos informáticos sostienen que las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que se interna en un sistema Informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente Informático es tema de controversia ya que para algunos dicho nivel no es indicador de delincuencia

Informática en tanto que otros aducen que los posibles delincuentes informáticos son personas hábiles, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen "delitos informáticos", estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año 1943.

Sutherland conocido criminólogo señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no se encontraban tipificadas en los ordenamientos jurídicos como Delitos informáticos, dentro de las cuales cabe destacar las violaciones a las leyes de patentes y fábrica, así como las de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas y la corrupción de altos funcionarios, entre otros.

Asimismo, el criminólogo norteamericano dice que tanto la definición de los "delitos informáticos" como la de los "delitos de cuello blanco" no son de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común

que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Es difícil elaborar estadísticas sobre ambos tipos de delitos. La "cifra negra" es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico de quienes los cometen, pero los daños económicos son altísimos; existe una gran Indiferencia de la opinión pública sobre los daños ocasionados a la sociedad: ésta no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables". Otra Coincidencia que tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativo de la libertad.

Por otra parte se considera que a pesar de que los "delitos informáticos" no poseen todas las características de los "delitos de cuello blanco", si coinciden en un número importante de ellas, aunque es necesario señalar que estas aseveraciones pueden y deben ser objeto ríe un estudio más profundo[6].

[6] INTRODUCCIÓN A LOS DELITOS INFORMÁTICOS, TIPOS Y LEGISLACIÓN, Publicado en el VI Congreso Latinoamericano en 1998, en Colonia, Uruguay, con la autorización del Autor/es Ricardo Revene (nieto) y Alicia Chiaravalleti, documento bajado de la URL: http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml.

1.6.2 Sujeto Pasivo. En primer término se tiene que distinguir que el sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos", mediante él se pueden conocer los diferentes ilícitos que cometen los delincuentes informáticos, que generalmente son descubiertos casuísticamente debido al desconocimiento del modus operandi. En segundo término otro sujeto pasivo de esta conducta es aquella persona que por falta de conocimientos acerca del debido uso de la red se convierte en una víctima potencial para estos delincuentes de la informática, que con artimañas y engaños logran obtener datos de la victima para luego estafarlos o utilizar sus datos en otras actividades ilícitas. Teniendo en cuenta lo antes mencionado se podría concluir que el sujeto pasivo en estas conductas es totalmente indeterminado.

Ha sido imposible conocer la verdadera magnitud de los "delitos informáticos" ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables; que sumado al temor de las empresas de denunciar este tipo de ilícitos por el desprestigio y su consecuente pérdida económica que esto pudiera ocasionar hace que éste tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra"[7].

7 Ibíd. http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml

2. ANTECEDENTE LEGISLATIVO DEL DELITO INFORMÁTICO

En el contexto internacional, se encuentra que son pocos los países que de manera expresa, clara y completa, cuenten con una legislación sobre este tema. Más sin embargo existen otros que ya han dado los primeros pasos en el tema y actualmente cuentan con una serie de normas que tratan y regulan la materia. Entre ellos, se destacan, Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, España, Argentina y Chile.

A continuación se mencionan los aspectos más importantes sobre las Leyes en los diferentes países, sobre la protección de bienes jurídicos afectados por los delitos Informáticos.

2.1 ALEMANIA

Este país cuenta con varias normas, de las cuales sobresale la siguiente; SEGUNDA LEY PARA LA LUCHA CONTRA LA CRIMINALIDAD ECONÓMICA DE 15 DE MAYO DE 1986[*].

[*] ALEMANIA. EL BUNDESTAG, (Parlamento Alemán) República Federal de Alemania. Disponible en http://www.delitosinformaticos.com/delitos/delitosinformaticos/legislacionalemana.shtml

Art. 202 y siguientes. Espionaje de datos. Al respecto esta ley contempla lo Siguiente:

“Quien sin autorización se procure a sí mismo o procure a otro datos especialmente asegurados contra ilícitas intromisiones, será castigado con pena privativa de libertad de hasta tres años o con pena de multa”.

“Se consideran datos, en el sentido del párrafo (1), solo aquellos electrónicos, magnéticos o que están almacenados de forma no inmediatamente perceptible o que son transmitidos”.

Art. 263 y siguientes. Estafa informática:

“Quien con la intención de conseguir una ventaja patrimonial ilícita, para sí mismo o para otro, cause un perjuicio patrimonial a un tercero, influyendo sobre el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o influyendo en la elaboración a través de una intervención ilícita, será castigado con pena privativa de libertad de hasta cinco años o con pena de multa”.

Art. 303 b y siguientes. Sabotaje informático:

“Quien destruya una elaboración de datos de especial significado para una fábrica ajena, una empresa ajena o una administración pública a través de la

comisión del tipo previsto en el Art. 303 a, par. 1° o por la destrucción, deterioro, inutilización, eliminación o alteración de un sistema de elaboración de datos o De los portadores de los datos, será castigado con pena privativa de la libertad de hasta cinco años o con pena de multe. La tentativa es punible".

2.2 AUSTRIA

Austria no tiene mayor legislación sobre este tema, sin embargo se destaca la Ley de reforma del Código Penal[*], sancionada el 22 de Diciembre de 1987, que sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes comenten este hecho utilizando su profesión de especialistas en sistemas.

2.3 FRANCIA

[*] AUSTRIA.LUNDTAG, (Legislatura Austríaca) República Federal de Austria.
Disponible en http://www.delitosinformaticos.com/delitos/delitosinformaticos/legislacionaustriaca.shtml

Francia cuenta con la Ley No. 88-19 de 5 de enero de 1988[*] sobre el fraude informático, y en razón dice:

Art. 462-2 código penal. Acceso fraudulento a un sistema de elaboración de datos.

“Quien fraudulentamente acceda a todo o parte de un sistema de tratamiento automático de datos o se mantenga en el será castigado con prisión de dos meses a un año y con multa de 2.000 a 50.000 francos o con una de las dos penas”.

“Si de ello resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema, la prisión será de dos meses a dos años y la multa de 10.000 a 100.000 francos”.

Art. 462-3 código penal. Sabotaje informático.

“Quien intencionalmente y con menosprecio de los derechos de los demás, impida o falsee el funcionamiento de un sistema de tratamiento automático de datos será castigado con prisión de tres meses a tres años y con multa de 10.000 francos o con una de las dos penas”

[*] FRANCIA.CONGRES DU PARLAMENT FRANCAIS, (El Congreso del Parlamento Francés). Disponible en http://www.delitosinformaticos.com/delitos/delitosinformaticos/legislacionfrancesa.shtml

Art. 462-4 código pena. Destrucción de datos.

"Quien intencionalmente y con menosprecio de los derechos de los demás, introduzca daños en un sistema de tratamiento automático de datos suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión, será castigado con prisión de tres meses a tres años y con multa de 2.000 a 500.000 francos o con una multa de las dos penas".

2.4 ESTADOS UNIDOS

Se debe tener en cuenta que este es uno de los países en donde se presenta la vulneración de bienes jurídicos con más frecuencia, debido a su gran desarrollo en tecnologías dado a su cultura vanguardista, lo que permite que a través de los medios computarizados y de Internet, se comentan miles de delitos, por tal motivo cuenta con una normatividad para enfrentar estas conductas, normas que de manera abreviada se referencian.

Estados Unidos adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986[*].

[*] ESTADOS UNIDOS.UNITED STATE SENATE, (Congreso Estadounidense). Estados Unidos de América Disponible en http://www.delitosinformaticos.com/delitos/delitosinformaticos/legislacioneeuu.shtml

Con la finalidad de eliminar los argumentos híper-técnicos acerca de qué es y que no es un virus informático, un gusano informático, un caballo de Troya (troyano) y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas. La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

En el mes de Julio del año 2000, el Senado y la Cámara de Representantes de este país tras un año largo de deliberaciones establece el Acta de Firmas Electrónicas en el Comercio Global y Nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos. Mensajes electrónicos y contratos establecidos mediante internet entre empresas y entre empresas y consumidores.

2.5 ESPAÑA

En el país ibérico, los delitos informáticos son un hecho sancionable por el Código Penal en el que el delincuente utiliza, para su comisión, cualquier medio informático. Estos tienen la misma sanción que sus homólogos no informáticos. Por ejemplo, se aplica la misma sanción para una intromisión en el correo electrónico que para una intromisión en el correo postal.

El Tribunal Supremo emitió una sentencia el 12 de junio 2007[*] (recurso N° 2249/2006; resolución N° 533/2007) que confirmó las penas de prisión para un caso de estafa electrónica (phising).

2.6 MÉXICO

En México los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática ya sean que estén protegidos por algún mecanismo de seguridad, se consideran propiedad del Estado o de las instituciones que integran el sistema financiero son hechos sancionables por el Código Penal Federal en el titulo noveno capítulo I y II[*].

[*] España. (Congreso de los Diputados). República de España.
Disponible en http://www.delitosinformaticos.com/delitos/delitosinformaticos/legislacionespañola.shtml
[*] México. Congreso Mexicano, Cámara de Diputados. Código Penal Federal LXI Legislatura.
Disponible en http://www.delitosinformaticos.com/delitos/delitosinformaticos/legislacionmexicana.shtml

El artículo 167 Fr. VI del Código Penal Federal sanciona con prisión y multa al que dolosamente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos.

La reproducción no autorizada de programas informáticos o piratería está regulada en la Ley Federal del Derecho de Autor en el artículo 11. También existen leyes locales en el código penal del Distrito Federal y el código penal del estado de Sinaloa.

2.7 VENEZUELA

Este país concibe como bien jurídico la protección de los sistemas informáticos que contienen, procesan, resguardan y transmiten la información. Están contemplados en la Ley Espacial contra los Delitos informáticos, de 30 de octubre de 2001[*].

La ley tipifica cinco clases de delitos:

[*] Venezuela. Congreso Nacional Venezolano. Reforma al Código Penal Federal. República de Venezuela Disponible en http://www.gobiernodevenezuela/seguridadpublica/legislacionactual.shtml

Contra los sistemas que utilizan tecnologías de información: acceso indebido (Art. 6); sabotaje o daño a sistemas (Art. 7); favorecimiento culposos del sabotaje o daño. (Art. 8): acceso indebido o sabotaje a -sistemas protegidos (Art. 9); posesión de equipos o prestación de servicios de sabotaje (Art. 10); espionaje informático (Art. 11); falsificación de documentos (Art. 12).

Contra la propiedad: hurto (Art. 13); fraude (Art. 14); obtención indebida de bienes o servicios (Art. 15); manejo fraudulento de tarjetas inteligentes o instrumentos análogos (Art. 16); apropiación de tarjetas inteligentes o instrumentos análogos (Art. 17): provisión indebida de bienes o servicios (Art. 18); posesión de equipo para falsificaciones (Art. 19).

Contra la privacidad de las personas y de las comunicaciones: violación de la privacidad de la data o información de carácter personal (Art. 20), violación de la privacidad de las Comunicaciones (Art. 21); revelación indebida de data o información de carácter personal (Art. 22); Contra niños y adolescentes: difusión o exhibición de material pornográfico (Art. 23); exhibición pornográfica de niños o adolescentes {Art. 24); Contra el orden económico, apropiación de propiedad intelectual (Art- 25); oferta engañosa (Art. 26).

3. EL DERECHO PENAL FRENTE A LOS DELITOS INFORMÁTICOS.

El acelerado crecimiento del uso de las computadoras ha dado lugar a un gran fenómeno de espacios nuevos y desconocidos llamados delitos informáticos, todo esto como consecuencia del desarrollo que ha tenido la tecnología informática, que a su vez ha abierto las puertas a un sin número de nuevas posibilidades de delincuencia, que muy seguramente en épocas anteriores era algo que no se dimensionaba.

El manejo fraudulento de computadores con ánimo de obtener algún lucro: la destrucción de programas o datos, el acceso y la utilización indebida de información, que puede afectar a la esfera de la privacidad, son algunos, entre otros problemas, a los cuales se aludirá simplemente, por cuanto constituyen procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos, o causar importantes daños materiales y morales.

Pero no solo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Estas conductas muestran una delincuencia de especialistas que generalmente es proceden de los mismos empleados encargados de la

informática, que en muchas ocasiones son capaces de borrar toda huella de los hechos. Lo anterior explicaría entonces como, en muchas oportunidades, el proceso investigativo referente a la realización de delitos informáticos se agrava por el hecho de que las variaciones del programa y de los datos no dejan huellas semejantes a las de las clásicas falsificaciones de documentos.

De acuerdo con el concepto elaborado por un grupo de expertos, invitados por la OCDE (Organización para la Cooperación y el Desarrollo Económico), que es una organización de cooperación internacional, compuesta por 34 Estados, cuyo objetivo es coordinar sus políticas económicas y sociales, con sede en Paris Francia y fundada en 1960, el termino delitos electrónicos, delitos vinculados con los ordenadores o llamados también (computer crime), se definen “como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o trasmisiones de datos”. La amplitud de este concepto es ventajosa, puesto que permite el uso de las mismas hipótesis de trabajo para todas clases de estudios ya sean penales, criminólogos, económicos, legales o preventivos.

La utilización de un bien inmaterial, como lo es la información, conlleva una serie de consecuencias. Así por ejemplo, el implantar un programa para infringir, mediante el uso de una computadora, hace que el objetivo con el cual se realiza el ilícito sea también inmaterial.

Bastaba considerar, al efecto, la concepción "materialista" del Código Penal., es decir, la exigencia de una cosa para la configuración de ciertos delitos, que era una de las fuentes de su superada inadecuación. Por ejemplo, el delito de daño no se aplicaba en relación con bienes intangibles. Por tanto, cuando un dato o conjunto de datos era destruido dolosamente, no habría delito, por más que se causara un perjuicio irremediable, que puede ser tan o más grave que en el caso de bienes materiales. Lo mismo se aplicaba al caso de la sustracción de datos, la cual no podía ser calificada como hurto.

El derecho penal era ineficaz ante este nuevo fenómeno como lo eran los delitos informáticos, por cuanto surgían una serie de vacios jurídicos debido a la falta de una legislación concreta y acorde a la realidad que se presentaba.

En este orden de ideas la realización de un acto fraudulento informático presentaba ciertas dificultades especiales, debido a que, como bien se sabe, el tipo penal que describe la estafa requiere la existencia de un sujeto pasivo del artificio o engaño. Este requerimiento que no existe en ciertos regímenes jurídicos como en el nuestro, hacía imposible, por la atipicidad, que se pudieran sancionar aquellos casos en los cuales el delincuente opera desde la computadora o maniobra el sistema, en forma tal que se causa el perjuicio.

Otros supuestos que requerirían probablemente un tratamiento legislativo especial, era el caso de la falsificación de documentos electrónicos, y el acceso no autorizado a sistemas informáticos.

Existían entonces otros tantos casos que eran verdaderamente raros, como la elaboración de una "bomba de tiempo"; que es un programa de computación, por el cual todo un sistema puede desaparecer (se refiere al soporte lógico del sistema, el llamado software) e incluso, dañar el soporte físico (hardware).

Al respecto, se señalan algunos de los nuevos fenómenos informáticos lesivos y entre otras, las técnicas relacionadas con la introducción de datos falsos: el llamado caballo de Troya, la técnica del salami, las puertas falsas, las bombas lógicas; la recogida de información residual, las chuzadas telefónicas, la simulación de sitios web y demás artimañas electrónicas que, desde la soledad de sus habitaciones y equipados tan solo de un computador personal, un modem y una gran imaginación, son capaces de acceder a través de una red pública de datos, al sistema informático de una empresa, institución bancaria, etc., para lograr la información confidencial, sustraerla, alterarla, distribuirla, o incluso preparar las condiciones para en ese momento, o posteriormente, efectuar un fraude.

Ante el caos delincuencial de grandes proporciones, que amenazaba con crecer muchísimo más, el legislador optó por enfrentar este fenómeno social de una forma directa e implacable que pudiera apaciguar el descontrolado crecimiento del delito informático dentro de la sociedad, que yacía sometida por decirlo de alguna manera a este flagelo invisible.

3.1 EL DELITO INFORMÁTICO EN COLOMBIA, LUCHA CONTRA LAS INSUFICIENCIAS REGULATIVAS.

Que la sociedad de gran manera es y será dependiente de la informática en general, como se observa hoy en día, explica de manera clara y sencilla la necesidad que tenía el derecho penal de ocuparse de varias conductas que ciertamente son lesivas al interés general de la comunidad y que no se tenían contempladas en el ordenamiento jurídico colombiano.

Este vacío normativo que se presentaba en el momento acarreó consigo una ola de pronunciamientos por parte de grandes autores estudiosos del tópico de los delitos informáticos. Los primeros elementos teóricos para el conocimiento de la disciplina y para una mejor comprensión de la misma, lo aporta Alexander Díaz García[8], al sostener cuales son los elementos esenciales para el estudio

[8] Op. Cit. DIAZ GARCIA, Alexander.

del Delito Informático, ello es así, si se miran los avances de la ciencia, pero que no llegan a la realidad en un Estado como el Colombiano, en donde la tecnología no esta tan masificada como en los Estados del primer mundo, esta teoría entonces tiene una mejor aplicación en los Estados avanzados donde la justicia tiene una amplia gama de elementos para la investigación compleja de los delitos informáticos, la tesis expuesta por este autor es mas para un sistema de investigación avanzado en aspectos tecnológicos, como los Europeos y el Norteamericano, pero para Colombia que apenas está comenzando a dar pasos en esta materia, es un arduo trabajo el que queda por hacer, teniendo en cuenta un sin número de factores que entorpecen dicho avance.

Otro grano de arena en este complejo tema lo aporta el Profesor y Honorable Ex Ministro de Justicia, Jaime Giraldo Ángel[9] en su trabajo Informática Jurídica Documental, explora la trama jurídica desde la validez de los documentos más usuales en Colombia y la validez de los mismos cuando son usados en forma electrónica, algo sirve esto para el estudio desde el área penal, mirando las causales de la falsedad, pero como no todos los delitos que se cometen en la informática hacen relación a este tipo Penal entonces se mirará con beneficio de inventario lo que aquí se dice. Para este ilustre doctrinante, los delitos informáticos comienzan desde el envió de los documentos que al darle validez a los mismos por parte de la Corte Constitucional, se está configurando una

[9] GIRALDO ANGEL, Jaime. Informática Jurídica Documental. Editorial Temis. Bogotá. 1999.

conducta que debe ser protegida y sancionada por el ordenamiento vigente, para este autor entonces la problemática nace en el mismo momento en que se reglamenta la validez de los documentos electrónicos, allí debió también a su juicio iniciarse un proceso de reglamentación para evitar la comisión de delitos desde la informática.

La recopilación de textos informáticos que hace Raymond Horte Martínez[10], desde su punto de vista sociológico, es mas en un contexto explorativo, desde la disciplina socio-jurídica, ya que analiza las implicaciones que los diversos autores recogidos por él tienen sobre esta conducta perjudicial para la sociedad de hoy. El análisis es mas critico que jurídico, pero sirve a la labor para vislumbrar desde esta disciplina auxiliar del Derecho, que aportes hay para el trabajo y como contrastar los diversos fenómenos que se presentan en materia de delito informático.

Las dimensiones de la Informática en el Derecho arrancan en el medio con el estudio presentado en 1995 a la comunidad jurídica Nacional por Abelardo Rivera Llanos[11], en su trabajo se comienzan después de la Constitución de 1991 a hablar por primera vez de la importancia que reviste para la Rama del Derecho, el conocimiento de la Tecnología de la Información y la Comunicación,

[10] HORTE MARTINÉZ, Raymond. Ciber-terrorismo Alfa-Redí. Revista de Derecho Informático, Edición Electrónica No. 082. Mayo de 2005.
[11] RIVERA LLANOS, Abelardo. Dimensiones de la Informática en el Derecho. (Perspectivas y Problemas) Ediciones Jurídicas Radar, Bogotá.1999.

la gran ayuda que este desarrollo tecnológico podría traerle a la dimensión jurídica nacional, entonces se trae a colación este trabajo por lo importante que es para el Derecho el tener un punto de partida, una primera piedra en la transformación del conocimiento a través del uso de una herramienta novedosa y necesaria, la que posteriormente se convirtió en un a ayuda de primer nivel y centro de estudio de la disciplina jurídica en Colombia.

Una valiosa contribución desde la Doctrina, la hace la Universidad Externado de Colombia[12], al reunir para un texto de Derecho Penal y Criminología a lo más granado de sus docentes expertos en esta materia para que desde su quehacer como investigadores y duchos en la materia aportaran luces al conocimiento de los Delitos Informáticos, no solo desde la norma sustancial punitiva sino también desde la procedimental y del porque se cometen esta clase de conductas punibles que son altamente lesivas a la sociedad. Este estudio es novedoso porque recoge conceptos básicos importantes a la hora de aplicar justicia por parte de los operadores judiciales del país y también por parte de los abogados al momento de hacer sus propias investigaciones para la solución de problemas o de emitir conceptos en asuntos concretos de esta rama del saber desde lo jurídico.

[12] UNIVERSIDAD EXTERNADO DE COLOMBIA. Revista.Derecho Penal y Criminología. Volumen XXVIII. No. 84. Bogotá. Mayo-Agosto 2007

Desde la Editorial Mac Graw Hill[13] se hace una aproximación al Delito Informático ya en concreto, se analizan las diferentes conductas que pueden ser cometidas por las personas desde un computador, esta novedosa tesis se expone en Colombia comenzando la legislación y sirve también de marco referencial a los trabajos que sobre esta materia se hacen a partir del mismo, además se innova en esta área porque se presenta una visión no desde lo sociológico, sino directamente desde lo jurídico, no desde lo Criminológico pero si desde lo legal de prima-facie para que las normas se sigan aplicando por parte de los estudiosos del tema y se tenga una herramienta importante de trabajo.

3.2 TENDENCIAS JURÍDICAS DOCTRINALES ACERCA DE LA ESTAFA A NIVEL MUNDIAL

El tema de la defraudación mediante la utilización de medios informáticos, es un tema que mantiene dividida a la doctrina que se ocupó en la materia, ya que para algunos es una situación que encuadra en la Estafa Genérica, sin necesidad de entrar a estudiar reforma alguna, ya que es innecesaria, de modo tal que la estafa informática, es una estafa genérica, que solo se diferencia de la otra en que el medio utilizado es un medio informático, ya que lo que se tiene en cuenta es el fin. Así estudiado y encarado el tema, no cabe duda al respecto,

[13]Op. Cit. TELLEZ VALDEZ, Julio.

pero no se debe agotar el tema en el estudio del fin, sino también debe abarcar las consecuencias, motivos y razones que llevan a la comisión de un hecho delictivo determinado.

Analizando la otra postura de la doctrina en la que se considera como un delito perfecto e independiente a la Estafa Informática, se advierte que esta postura doctrinaria sostiene que si bien el fin del delincuente, es un fin defraudatorio, y para ello el delincuente se vale de cualquier medio, hace la gran diferencia de que el medio utilizado es un medio informático, en donde en la mayoría de los negocios jurídicos y económicos que se celebran, existe una relación de marcada y determinante superioridad, ya que el soporte informático, se abastece de redes que en determinadas ocasiones tienen un respaldo mundial, que los deja en una situación de supremacía y dominio de las acciones, lo que desvirtúa la igualdad en las negociaciones. Pero en el punto que se hace hincapié es en la casi total desinformación y la ausencia de conocimientos necesarios para tomar los recaudos y las medidas preventivas tendientes a asegurar la integridad de su propio patrimonio.

De modo tal que la desinformación es el elemento clave utilizado por los delincuentes, ya que en determinadas ocasiones, es de tal envergadura, que resulta repugnante para la justicia el aprovechamiento de la víctima por parte del delincuente. Respecto a éste punto, cabe resaltar, es que se debe tener

cuidado con la utilización que se le da al término "Desinformación o Desconocimiento", ya que entraría el interrogante planteado acerca si se configura el delito cometido contra una persona que tiene grandes conocimientos en informática. Pero en lo que atañe a la clasificación autónoma de esta forma estafatoria, se comparte el criterio de la segunda posición doctrinaria, pero no ya allanándose a los argumentos antes vertidos, sino agregándole el complemento que es con un medio específico, lo que encuadra en una defraudación especial, ya que se cometió con un método particular.

Internet se ha convertido en un medio muy susceptible a la comisión de estafas, debido a la escasa seguridad que todavía aporta la Red y a la pericia de muchos sujetos entendidos en el tema y que no dudan de aprovechar sus conocimientos en beneficio propio perjudicando a terceros.

En algunos sitios web en Internet te piden los datos de tu tarjeta de crédito con la excusa de comprobar si eres mayor de edad, y si el sujeto no cae en cuenta de que con este número no es posible conocer la edad del titular de la misma, tiene un problema porque lo más probable es que lo estafen.

En otros sitios (sites), como algunos de subastas, muestran una fotografía del producto que subastan, por ejemplo un Rolex, y tras pujar por ejemplo; lo adquieres, y cuando te llega a tu casa el paquete y/o abres compruebas con

cara de espanto que no se trata de un reloj sino de su fotografía, tal y como se veía en su página.

Además, la estafa se produce cuando en un sitio de contenido para adultos te ofrecen visualizar las imágenes gratis tras descargar un programa necesario para ello. Este es el caso del sitio sexygiris.com, cuyos usuarios se descargaron un visor de imágenes que en realidad era un Caballo de Troya, que silenciaba el módem del usuario y lo desconectaba de su proveedor de acceso a Internet y lo conectaba a un número de teléfono de Moldavia (antigua Unión Soviética), desde donde se redirigía la llamada a Norteamérica, donde se encontraban las imágenes solicitadas por el internauta. La factura telefónica alcanzaba cifras astronómicas ya que, aunque el sujeto abandonara el sitio, continuaba conectado a Moldavia.

4. ACTUALIDAD LEGAL EN MATERIA DE DERECHO INFORMÁTICO EN COLOMBIA: EVOLUCION LEGISLATIVA

En este capítulo se observa el arduo proceso al que se enfrentó la legislación colombiana, la cual tenía la necesidad de satisfacer las insuficiencias que suscitaban en la sociedad debido al avance de las tecnologías y el ritmo acelerado del proceso de globalización de la información en todo el mundo. Si es bien sabido que los delitos pertenecientes a la informática, tienen en si un carácter multiofensivo, en el sentido de que estos pueden afectar varios bienes jurídicos tutelados, tales como lo son la intimidad personal, el patrimonio económico de las personas y la fe pública, esto significaba que el legislador penetraría con su intervención varias esferas del desarrollo social con respecto a la regulación de conductas que anteriormente no se entendían como delitos.

4.1 LEY 527 DE 1999

Ley 527 de 1999 (Acceso y uso de mensajes de datos, comercio electrónico, firmas digitales y entidades certificadoras).

La ley de comercio electrónico sancionada por el Gobierno Nacional, no contribuye a crear una nueva forma de hacer comercio. La Ley no crea el comercio electrónico ni pretende hacerlo, este de por sí ya existe, la ley sólo es

la respuesta a una realidad mercantil que cada día tiene mayor acogida en todos los niveles y en todos los Estados. Se caracteriza, entre otras cosas, porque:

- No existe contacto físico entre los sujetos intervinientes.
- El espacio en que se realizan las operaciones es virtual
- No hay horarios, lo que permite realizar las operaciones en tiempo real.

Es importante mencionar cuales han sido los antecedentes que fueron tenidos en cuenta por el Gobierno Nacional al presentar esta iniciativa al Congreso de la República.

Es palpable que el comercio electrónico constituye una realidad mercantil, en 1991 había 4.5 millones de usuarios de Internet, en 1998 eran 100 millones, y para el año 2012 se calcula que tendrá 820 millones de usuarios.

Se calcula que el comercio electrónico es de 8 billones de dólares, las proyecciones para el año 2012 indican que este oscilara entre 100 y 400 billones de dólares.

Colombia no se ha sustraído del impacto mundial producido por el comercio electrónico y con gran esfuerzo sus empresarios y ciudadanos se han introducido en este mundo sin barreras, realizando desde hace varios años transacciones comerciales por esta vía.

La realidad del comercio electrónico en el mundo y, su elevado y rápido desarrollo originó preocupación en los foros de discusión sobre temas del derecho, con relación a la situación jurídica de este tipo de transacciones, y a las herramientas jurídicas con que contaba el empresario o el ciudadano corriente si por hacer uso del comercio electrónico y de las bondades de no utilizar papel, contrataba con el sujeto equivocado, o no recibía la bicicleta sino unos patines, ¿Cómo asegurarse que su negocio no correría riesgo alguno? ¿Ante quién podría acudir? ¿Cómo solucionaría su problema?

Era necesario crear herramientas jurídicas de defensa y garantía para los usuarios del comercio electrónico y de otros mecanismos, que por agilizar las comunicaciones se alejaban de los formalismos legales establecidos.

Esta realidad y necesidad fueron tenidas en cuenta por la Comisión de Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI o UNCITRAL), seno en el cual participan 30 Estados nombrados por la Asamblea

General por un periodo determinado y en el cual se discuten asuntos relacionados con el derecho mercantil internacional.

Lo que la llevó a reunir expertos y formular una Ley modelo en el tema de comercio electrónico, que permitiera a los Estados adecuarla a sus ordenamientos internos y procurar así la uniformidad internacional.

Usualmente la CNUDMI puede producir leyes modelos y convenciones. Sin embargo, en este tema a consideró más conveniente hacer uso de la ley modelo, de tal forma que los Estados que la adoptasen, acondicionaran sus legislaciones y ordenamientos internos conforme con sus necesidades, lo que permitió que Colombia lo hiciera con el suyo.

El comercio electrónico no está desarrollado de la misma forma en todos los Estados, razón por la que no era conveniente realizar una convención.

De aquellas discusiones en el ámbito internacional, en las que participó Colombia se llegó a la conclusión sobre la necesidad de crear un ordenamiento con disposiciones minimalistas, que no entorpeciera el desarrollo del comercio dado a través de estos medios, pero que diera seguridad y garantía a las operaciones realizadas en línea.

La ley modelo de comercio electrónico fue tenida en cuenta por Colombia y el gobierno integró una comisión de trabajo sobre la misma, cuyo objetivo era redactar y acondicionar las propuestas de dicha ley a nuestra legislación.

Esa Comisión estuvo integrada por los Ministerios de Justicia y el Derecho, Transporte, Desarrollo y Comercio Exterior, y en las discusiones participaron otros entes gubernamentales y privados como el Incomex, el Banco de la República, las Empresas Publicas de Medellín, la Cámara de Comercio de Bogotá entre otros.

De allí el Gobierno Nacional presentó el proyecto al Congreso de la República y, para llegar al proyecto definitivo, se tuvieron en cuenta los siguientes objetivos:

Eliminar los obstáculos mercantiles y procurar un marco legal seguro donde las transacciones se den en un ámbito confiable.

Contribuir con la armonización jurídica, lo que permitiría que las disposiciones mínimas y lo propuesto por la ley modelo tuvieran una aplicación universal sin necesidad de una convención.

Esto mismo generaría que se tuvieran mecanismos ágiles de interpretación y se promoviera la economía y la eficiencia del comercio internacional.

Aunque no se tiene una definición exacta y nuestra ley contiene una bastante precisa, podría entenderse el comercio electrónico como la técnica o modalidad mercantil realizada mediante el intercambio electrónico de una propuesta y una aceptación por personas distantes, evitando así, el tradicional intercambio de documentos escritos dando lugar al llamado contrato electrónico o mejor definido como contrato telemático.

Esta definición es bastante amplia y cobija muchos medios de comunicación, tiene, además, presentes las diversas técnicas de comunicación y no excluye, sino que cobija, toda eventual innovación tecnológica.

De esta forma, fue expedida la Ley 527 de 1999 mediante la cual se define y reglamenta el acceso y uso de los mensajes de datos el comercio electrónico, las firmas digitales y se establecen las entidades de certificación, entre otras disposiciones.

El objeto principal pero no el único, de la ley de comercio electrónico es de dotar de seguridad jurídica las transacciones y operaciones realizadas a través de mensajes de datos.

No es el único porque la ley contribuye a brindar herramientas útiles para el uso del comercio electrónico, pero es el principal porque el comercio electrónico es una realidad, que necesita tener un respaldo jurídico, así como certeza y seguridad necesarias para que se realicen operaciones confiables.

La ley, como es obvio, no resuelve todos los problemas que puedan suscitarse en el desarrollo de esta modalidad de comercio, pero trata de otorgar cierta tranquilidad y reconocimiento jurídico a los actores que en ella intervienen. Depende del uso que se haga de las herramientas que brinda la ley[14].

4.2 LEY 599 DEL 2000

Como se planteó en el Capítulo I de esta investigación, el Código Penal Colombiano no hacía referencia como tal, de los delitos informáticos, mas sin embargo algunos de sus artículos protegen algunos bienes jurídicos, que son vulnerados por algunas acciones cometidas a través de la red informática, a continuación algunos ejemplos claros de la tipificación de algunas conductas.

El Art. 192: Violación ilícita de comunicaciones, exige ilicitud en el acceso a la información, esto es, no demanda específicamente la vulneración de medidas

[14] Articulo descargado de la página de Internet
http://sabanet.unisabana.edu.co/comercio/comentarios_ley_de_comercio_elec.htm

de seguridad, por lo que cabe preguntarse si en el giro "ilícitamente" cabe entender la trasgresión de normas de seguridad.

Esta interpretación se ahorra en frente del art. 195: Acceso abusivo a un sistema informático (Derogado ley 1273 de 2009). Pues, allí se demanda la protección con medida de seguridad.

Asimismo, dentro del mentado art 192, se castiga la interceptación ilícita no autorizada de datos y que se encuentran protegidos por el derecho a la intimidad; asimismo, se castiga la violación del derecho a la reserva y confidencialidad de los datos privados. La norma carece de referentes de ánimo o de la exigencia de causación de perjuicios concretos, para su castigo.

El Art. 192, sanciona la conducta de destruir comunicaciones privadas; empero, el daño a los datos contenidos en el sistema informático, no podrá condenarse por la vía del art. 265 del CP. El cual consagra el delito de daño en bien ajeno, oponiendo castigo a quien destruya inutilice, haga desaparecer o del cualquier otro modo dañe bien ajeno, mueble o inmueble.

Como quiera que los datos, prima facies, no son "bienes mueble o inmuebles", las conductas de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización datos informáticos, no parecen encuadrables en esta disposición ni

tampoco en el art. 357: Daño en obra o elementos de los servicios de comunicaciones, energía y combustibles. Tipo destinado a proteger soportes materiales de ciertos servicios en el ámbito de la seguridad pública. Igualmente, tampoco parece encuadrable típicamente la conducta de obstaculizar el funcionamiento de un sistema informático.

En el art, 199: Sabotaje. Consagró el legislador, una especial conducta de sabotaje, en la cual se castiga la destrucción de datos y soportes lógicos, pero habida cuenta del bien jurídico protegido "la libertad de trabajo y asociación", el dicho tipo especial de daño, solo es punible en ese específico y claro ámbito, conformidad de que la conducta de dañar o destruir datos o soportes lógicos debe ser con el fin de suspender o paralizar el trabajo.

Respecto de las infracciones que aluden a la falsedad y la estafa, la redacción del art. 294: Documento. Al prever que es documento para efectos penales, también, el soporte material que exprese o incorpore datos o hechos, que tengan capacidad probatoria, bien permite concluir que es posible incurrir en cualquiera de los delitos de la rúbrica sea por la introducción, alteración, o por otra parte es claro que en la redacción del art. 246: De la estafa. “El que. obtenga provecho ilícito para sí o para un tercero, con perjuicio ajeno, induciendo o manteniendo a otro en error por medio de artificios o engaños” son perfectamente encuadrables las conductas tendientes a obtener una

defraudación patrimonial ajena, por medio de la introducción, alteración, borrado o supresión de datos informáticos, o en todo caso, por cualquier forma de atentado al funcionamiento de un sistema informático con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para terceros, pues, tal espectro es descifrable bajo el giro "induciendo o manteniendo a otro en error por medio de artificios o engaños". Borrado o supresión dolosa y sin autorización de datos informáticos.

El art. 218: Pornografía con personas menores de 18 años (Modificado ley 1236 de 2008), castiga con pena de prisión a quien fotografíe, filme, venda, compre, exhiba o de cualquier manera comercialice material pornográfico en el que participen menores de edad. Asimismo, está penado, según el art, 218-A (Modificado), quien utilice o facilite el correo tradicional, las reglas globales de información, o cualquier otro medio de comunicación para obtener contacto sexual con menores de dieciocho (18) años, para ofrecer servicios sexuales con estos.

Como sea lo anteriormente planteado, se observa entonces que ya había iniciado en la legislación domestica una tipificación respecto al tema de los delitos penales, pero se hacía obligatorio, como se ha planteado en capítulos anteriores y como se planteara en los posteriores, la necesidad de que se

incorporara en el Código Penal un capitulo que expresamente tipificara las conductas punibles que se cometen a través de estos medios.

4.3 LEY 603 DEL 2000

En Colombia existen leyes que protegen la piratería, entre las cuales se pueden destacar los artículos 271 y 272 del Código Penal, así como la Ley 603 de 2000.

Los artículos 271 y 272 del Código Penal establecen penas de 4 a 8 años de prisión y multas de 26 a 1000 salarios mínimos legales mensuales vigentes por la defraudación a los derechos patrimoniales de autor y la violación a los mecanismos de protección de derechos de autor, respectivamente.

La Ley 1032 de 2006, por medio de la cual se modifican los artículos 271 y 272 del Código penal, también introdujo modificaciones con las cuales se establecieron penas de prisión de 4 a 8 años y multas entre 26, 66 y 1.000 salarios mínimos legales mensuales vigentes para quienes violen los derechos patrimoniales de autor y los derechos conexos.

Según la Ley, estará en ese delito quien incurra en siete conductas entre las que figuran el alquiler o comercialización de fonogramas, videogramas,

programas de ordenador o soportes lógicos u obras cinematográficas y "retransmita, fije, reproduzca o, por cualquier medio sonoro o audiovisual, divulgue las emisiones de los organismos de radiodifusión" y "recepcione, difunda o distribuya por cualquier medio las emisiones de la televisión por suscripción", dice el texto de la ley.

Por su lado la Ley 603 de 2000, obliga a incluir en los informes de gestión una declaración sobre el cumplimiento de las normas sobre derechos de autor, y su violación puede conllevar a multas y otras sanciones administrativas.

4.4 CORTE CONSTITUCIONAL SENTENCIA 662 DE 8 DE JUNIO DE 2000

En el referido pronunciamiento jurídico se describirá de manera clara y precisa el desenvolvimiento de la controversia originada por entrada en vigencia de la Ley 527 de 1999 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

REF.: Expediente No. D-2693

Acción pública de inconstitucionalicidad contra la Ley 527 de 1999 y, particularmente sus artículos 10, 11, 12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45, "Por medio de la cual se define y

reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".

Actora: OLGA LUCIA TORO PÉREZ

Temas: El reconocimiento jurídico de la validez plena y del valor probatorio de los mensajes de datos. El Comercio Electrónico. La firma digital. Las entidades de certificación y la emisión de certificados sobre la autenticidad de los mensajes de datos y las firmas digitales. La actividad de las entidades de certificación y la función notarial. Magistrado Ponente: Dr. FABIO MORÓN DÍAZ

en el proceso instaurado por OLGA LUCIA TORO PÉREZ, en ejercicio de la acción pública de inconstitucionalidad, en contra de la Ley 527 de 1999 y, especialmente de los artículos 10, 11, 12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45 de la Ley 527 de 1999, "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".

La ciudadana OLGA LUCIA TORO PÉREZ, en ejercicio de la acción pública de inconstitucionalidad consagrada en la Constitución Política de 1991, pide a la Corte declarar inexequibles los artículos 10, 11, 12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45 de la Ley 527 de 1999.

El Magistrado Sustanciador mediante auto de noviembre diecinueve (19) del pasado año, admitió la demanda al haberse satisfecho los requisitos establecidos en el Decreto 2067 de 1991.

En defensa de la constitucionalidad de la Ley 527 de 1999 durante el término legal intervinieron, de manera conjunta, los ciudadanos Carolina Deyanira Urrego Moreno, Edgar Iván León Robayo, Jaír Femando ímbachí Cerón; los ciudadanos Carolina Pardo Cuéllar y Santiago Jaramillo Caro; el doctor Ramón Francisco Cárdenas, en representación de la Superintendencia de Industria y Comercio; los doctores María Clara Gutiérrez Gómez en representación del Ministerio de Comercio Exterior y José Camilo Guzmán Santos, como apoderado del Ministerio de Justicia; el doctor Carlos Blas Buraglia Gómez, en su condición de Presidente Ejecutivo (e) de la Cámara de Comercio de Bogotá; el doctor Garios César Rolón Bermúdez, en representación del Ministerio de Comunicaciones; los ciudadanos Eleonora Cuéllar Pineda y Sergio Pablo Michelsen Jaramillo, en representación de la Fundación Foro Alta Tecnología; y, el doctor Carlos Eduardo Sema Barbosa en representación del Ministerio de Desarrollo Económico.

Naciones Unidas para el Desarrollo del Derecho Mercantil internacional (CNUDMI).

En el caso Colombiano fue el producto de un proceso en el que participaron los sectores público y privado que tuvieron asiento en la Comisión Redactora de la que formaron también parte los Ministros de Justicia y del Derecho, Transporte, Desarrollo Económico y Comercio Exterior.

El Comercio Electrónico encierra dentro de su filosofía los postulados de la buena fe comercial y de la libertad contractual entre los negociantes, principios éstos que rigen todas y cada una de las transacciones realizadas mediante su utilización.

La regulación del Comercio Electrónico busca permitir el acceso de todas las personas a esta forma tecnológica de realizar transacciones de índole comercial y contractual.

Ni el comercio electrónico ni la actividad de las entidades de certificación son un servicio público, pues las partes no se encuentran en la obligación ni en la necesidad de solicitar los servicios de una entidad de certificación para la celebración de un negocio jurídico. Por el tipo de relaciones que regula, se trata de un asunto de la órbita del Derecho Privado que, por supuesto, precisa de un control estatal, que estará a cargo de la Superintendencia de Industria y Comercio, que vigila a las entidades de certificación desde el punto de vista técnico y operativo.

La ley cuestionada apunta a proveer tanto a los mensajes de datos como al comercio electrónico, la integridad, confiabilidad y la seguridad que en este tipo de intercambios electrónicos son cruciales, asimismo traían de operaciones y de transacciones en que las partes interactúan electrónicamente, a través de redes telemáticas, sin haber contacto directo o físico.

Las firmas digitales, el certificado electrónico, y el servicio de certificación que prestan las entidades de certificación son herramientas de índole eminentemente técnica que apuntan a dotar de seguridad los mensajes de datos y el comercio electrónico.

Los cargos de la demanda resultan infundados porque las entidades de certificación no prestan un servicio público y menos dan fe pública. Las entidades de certificación no son notarías electrónicas, pues no sustituyen ni prestan los mismos servicios, según se deduce de la sola lectura del artículo 30 de la Ley 527 de 1999 que relaciona las actividades que las primeras pueden realizar.

Consideraciones.

Es bien sabido que los progresos e innovaciones tecnológicas logrados principalmente durante las últimas décadas del siglo XX, en el campo de la tecnología de los ordenadores, telecomunicaciones y de los programas

informáticos, revolucionaron las comunicaciones gracias al surgimiento de redes de comunicaciones informáticas, las cuales han puesto a disposición de la humanidad, nuevos medios de intercambio y de comunicación de información como el correo electrónico, y de realización de operaciones comerciales a través del comercio electrónico.

En el capítulo I de la parte III, respecto de la aplicación específica de los requisitos jurídicos de los mensajes de datos, se encuentra la firma, y para efectos de su aplicación se entiende por firma digital:

"un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido vinculado a la clave criptográfica privada del iniciado, permite determinar que este valor numérico se ha obtenido exclusivamente con la clave criptográfica privada del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación". (Artículo 2°. Literal h).

A través de la firma digital se pretende garantizar que un mensaje de datos determinado proceda de una persona determinada; que ese mensaje no hubiera sido modificado desde su creación y transmisión y que el receptor no pudiera modificar el mensaje recibido.

Una de las formas para dar segundad a la validez en la creación y verificación de una firma digital es la Criptografía, la cual es una rama de las matemáticas aplicadas que se ocupa de transformar, mediante un procedimiento sencillo, mensajes en formas aparentemente ininteligibles y devolverías a su forma original.

Mediante el uso de un equipo físico especial, los operadores crean un par de códigos matemáticos, a saber: una clave secreta o privada, conocida únicamente por su autor, y una clave pública, conocida como del público. La firma digital es el resultado de la combinación de un código matemático creado por el iniciador para garantizar la singularidad de un mensaje en particular, que separa el mensaje de la firma digital y la integridad del mismo con la identidad de su autor.

De otra parte, la Corte encuentra que el artículo 4° del Decreto 266 del 2000, expedido por el Presidente de la República en ejercicio de las facultades extraordinarias conferidas por el numeral 5° del artículo 1° de la Ley 573 del 7 de febrero del 2000, conforma unidad normativa con el artículo 10 de la acusada Ley 527 de 1999, dada su identidad de contenido.

Ciertamente, el artículo 4° de la Ley 573 del 7 de febrero del 2000 dispone: Artículo 4°. Medios tecnológicos. Modificase el artículo 26 del decreto 2150 de 1995, el cual quedará así:

"Artículo 26. Medios tecnológicos Se autorizan a la Administración Pública el empleo de cualquier medio tecnológico o documento electrónico, que permita la realización de los principios de igualdad, economía, celeridad, imparcialidad, publicidad, moralidad y eficacia en la función administrativa, así como el establecimiento de condiciones y requisitos de seguridad que cada caso sean procedentes, sin perjuicio de las competencias que en la materia tengan algunas entidades especializadas.

Toda persona podrá en su relación con la administración hacer uso de cualquier medio técnico o electrónico, para presentar peticiones, quejas o reclamaciones ante las autoridades. Las entidades harán públicos los medios de que dispongan para permitir esta utilización. Los mensajes electrónicos de datos serán admisibles como medios de prueba y su fuerza probatoria será la otorgada en (as disposiciones del Capítulo VIII del Título XIII, Sección III Libro Segundo del Código de procedimiento Civil, siempre que sea posible verificar la identidad del remitente, así como la fecha de recibo del documento."

Por su parte el artículo 10 de la Ley 527 de 1999, preceptúa:

"Artículo 10. Admisibilidad y fuerza probatoria de los mensajes de datos. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y, probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original."

Por consiguiente y en vista de que se presenta el fenómeno jurídico de unidad de materia entre el artículo 10 de la Ley 527 de 1999 acusado y el artículo 4 del Decreto 266 del 2000 dictado con base en las facultades extraordinarias establecidas en la Ley 573 del 2000, pues regulan un mismo aspecto, esto es, el valor probatorio de los mensajes electrónicos, la Corte estima que la declaratoria de constitucionalidad comprenderá también al artículo 4° del Decreto 265 del 2000 por las razones atrás referidas.

Es pues, del caso, extender el pronunciamiento de exequibilidad, en cuanto hace al cargo examinado, también a la norma últimamente mencionada. Así se decidirá.

Decisión.

En mérito de lo expuesto, la Corte Constitucional, en nombre del pueblo y por mandato de la Constitución.

Resuelve:

Primero.- En cuanto a los cargos examinados, DECLÁRENSE EXEQUIBLES los artículos 10, 11, 12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45 de la Ley 527 de 1999.

Segundo.- Declarar EXEQUIBLE el artículo 4°. Del Decreto 266 del 2000 dictado en ejercicio de las facultades extraordinarias establecidas en la Ley 573 del 2000, conforme a la parte motiva de esta providencia.

4.5 LEY 679 DEL 2001

La Ley 679 del año 2001, entre otras cosas establece las normas atinentes para contrarrestar el abuso sexual de menores, a través de medios electrónicos.

En uno de sus artículos dice que el Instituto Colombiano de Bienestar Familiar conformará una comisión con el propósito de elaborar un catálogo de actos abusivos en el uso y aprovechamiento de redes globales de información en lo relacionado con menores de edad. Esta comisión propondrá iniciativas técnicas

como sistemas de detección, filtro, clasificación, eliminación y bloqueo de contenidos perjudiciales para menores de edad en las redes globales, que serán transmitidas al Gobierno Nacional con el propósito de dictar medidas en desarrollo de esa ley.

El inciso segundo del artículo 4° de la Ley 679 de 2001 estipula que esta comisión presentará un informe escrito al Gobierno Nacional, en el cual consten las conclusiones de su estudio, así como las recomendaciones propuestas;

En su artículo 5° de la Ley 679 de 2001 establece que de acuerdo a este informe, el Gobierno Nacional con el apoyo de la CRT, adoptará las medidas administrativas y técnicas desuñadas a prevenir el acceso de menores de edad a cualquier modalidad de información pornográfica, y a impedir el aprovechamiento de redes globales de información con fines de explotación sexual infantil u ofrecimiento de servicios comerciales que impliquen abuso sexual con menores de edad, reglamentar el artículo 5° de la Ley 679 de 2001, con el fin de establecer las medidas técnicas y administrativas destinadas a prevenir el acceso de menores de edad a cualquier modalidad de información pornográfica contenida en Internet o en las distintas clases de redes informáticas a las cuales se tenga acceso mediante redes globales de información.

Además a propender para que estos medios no sean aprovechados con fines de explotación sexual infantil u ofrecimiento de servicios comerciales que impliquen abuso sexual con menores de edad, cuya actividad u objeto social tenga relación directa o indirecta con la comercialización de bienes y servicios a través de redes globales de información.

La ley hace referencia a unas prohibiciones que deben tener los proveedores o servidores, administradores y usuarios de redes globales de información, y son las siguientes.

- Alojar en su propio sitio imágenes, textos, documentos o archivos audiovisuales que impliquen directa o indirectamente actividades sexuales con menores de edad.
- Alojar en su propio sitio material pornográfico, en especial en modo de imágenes o videos, cuando existan indicios de que las personas fotografiadas o filmadas son menores de edad.
- Alojar en su propio sitio vínculos o "links", sobre sitios telemáticos que contengan o distribuyan material pornográfico relativo a menores de edad.

Además plantea unos deberes y dice;

Sin perjuicio de la obligación de denuncia consagrada en la ley para todos los residentes en Colombia, los proveedores, administradores y usuarios de redes globales de información deberán:

- Denunciar ante las autoridades competentes cualquier acto criminal contra menores de edad de que tengan conocimiento, incluso de la difusión de materia pornográfico asociado a menores.
- Combatir con todos los medios técnicos a su alcance la difusión de material pornográfico con menores de edad.
- Abstenerse de usar las redes globales de información para divulgación de material ilegal con menores de edad.
- Establecer mecanismos técnicos de bloqueo

4.6 CORTE SUPREMA DE JUSTICIA, SALA DE CASACIÓN PENAL. SENTENCIA DEL 30 DE ABRIL DE 2008. PROCESO NO 29188.

Proceso No 29188. CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN PENAL. Magistrado Ponente Dr. JOSÉ LEÓNIDAS BUSTOS MARTÍNEZ Aprobado acta número 105.

Este fallo adquirió gran repercusión en muchos portales de Internet y varios medios periodísticos del mundo. El motivo de ello fue la postura que dejó

sentada la Corte Suprema de Colombia respecto de la descarga de música por Internet, más allá del conflicto puntual que fuera planteado en el recurso.

Así, el máximo tribunal sostuvo que "si en la Internet circuían millones de canciones, no puede concentrarse en el derecho penal la función de perseguir a los usuarios que, aprovechando tal circunstancia, descargan la música que se coloca a su alcance, pues en estos casos como en todos aquellos en los que la persona obra sin ánimo de lucro y sin el propósito de ocasionar perjuicio a la obra o a los intereses económicos del titular de los derechos, resulta imposible afirmar la existencia de una conducta punible, toda vez que no se lesiona o pone efectivamente en peligro el bien jurídica tutelado por la ley".

De este argumento se desprende que la Corte Suprema de Colombia entiende que deben acreditarse dos elementos fundamentales para que se configure el delito: el ánimo de lucro y la intención de ocasionar un perjuicio. En ese sentido, sostuvo que las conductas que le fueran imputadas al procesado y por las que fuera condenado en la instancia inferior duplicación de discos compactos y uso de software sin las respectivas licencias resultan atípicas cuando no existe intención de lucrar con ello ni propósito de ocasionar un perjuicio a los dueños de dichas obras.

Cabe resaltar, como punto sobresaliente del fallo la mención a la ausencia de reproducción a gran escala para su comercialización, que puede interpretarse como indicio de la falta de ánimo de lucro y de la intención de ocasionar un perjuicio. En igual sentido se expresa el Procurador, al señalar que las normas penales en este caso buscan reprimir lo que se conoce como "piratería", que sería el eje central de las campañas de la industria cultural y del entretenimiento, intentando con ello graficar que la conducta del imputado no alcanza tales dimensiones.

Resulta interesante observar que el máximo tribunal de Colombia, en este caso, consideró especialmente la realidad de una cultura digital amplia y de conductas socialmente aceptadas en consecuencia; y pretendió adecuar su resolución a dicha circunstancia.

4.7 LEY 1266 DE 2008 (LEY DE HABEAS DATA)

Esta ley no acarreó consecuencias en cuanto a la legislación penal actual vigente pero es de gran importancia señalarla debido a que entró a regular el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países, así como también se dictaron otras disposiciones en áreas en donde

existían muchos abusos por parte de las entidades financieras y centrales de riesgo.

Como la misma ley lo indica en su articulo primero, su objeto es “desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países”.

Esta ley también entró a definir los sujetos intervinientes dentro de la relación entidad usuario, que existe en el manejo de la información personal en la vida cotidiana, se delimitó entonces quien es el titular de la información, la fuente de información, el operador de la información y quien es el usuario en todo este engranaje comercial. También se precisaron conceptos que ya se manejaban pero que no estaban contemplados en anteriores normatividades como lo es el concepto de dato personal, dato público, dato privado, dato semiprivado.

De igual forma se establecieron los principios rectores de la administración de datos y la manera en la debe circular la información, asimismo se implantaron los mecanismos legales necesarios para la salvaguarda de los derechos de los usuarios y de las entidades, como versa en el artículo 16 que habla de las peticiones de consulta y reclamos en el que se señala lo siguiente: “ Los titulares de la información o sus causahabientes podrán consultar la información personal del titular, que repose en cualquier banco de datos, sea este del sector público o privado. El operador deberá suministrar a estos, debidamente identificados, toda la información contenida en el registro individual o que esté vinculada con la identificación del titular.

La petición, consulta de información se formulará verbalmente, por escrito, o por cualquier canal de comunicación, siempre y cuando se mantenga evidencia de la consulta por medios técnicos.

La petición o consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la petición o consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su petición, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

PARÁGRAFO. La petición o consulta se deberá atender de fondo, suministrando integralmente toda la información solicitada.

II. Trámite de reclamos. Los titulares de la información o sus causahabientes que consideren que la información contenida en su registro individual en un banco de datos debe ser objeto de corrección o actualización podrán presentar un reclamo ante el operador, el cual será tramitado bajo las siguientes reglas:

1. La petición o reclamo se formulará mediante escrito dirigido al operador del banco de datos, con la identificación del titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y si fuere el caso, acompañando los documentos de soporte que se quieran hacer valer. En caso de que el escrito resulte incompleto, se deberá oficiar al interesado para que subsane las fallas. Transcurrido un mes desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido de la reclamación o petición.

2. Una vez recibida la petición o reclamo completo el operador incluirá en el registro individual en un término no mayor a dos (2) días hábiles una leyenda que diga “reclamo en trámite” y la naturaleza del mismo. Dicha información deberá mantenerse hasta que el reclamo sea decidido y deberá incluirse en la información que se suministra a los usuarios.

3. El término máximo para atender la petición o reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender la petición dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su petición, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

4. En los casos en que exista una fuente de información independiente del operador, este último deberá dar traslado del reclamo a la fuente en un término máximo de dos (2) días hábiles, la cual deberá resolver e informar la respuesta al operador en un plazo máximo de diez (10) días hábiles. En todo caso, la respuesta deberá darse al titular por el operador en el término máximo de quince (15) días hábiles contados a partir del día siguiente a la fecha de presentación de la reclamación, prorrogables por ocho (8) días hábiles más, según lo indicado en el numeral anterior. Si el reclamo es presentado ante la fuente, esta procederá a resolver directamente el reclamo, pero deberá informar al operador sobre la recepción del reclamo dentro de los dos (2) días hábiles siguientes a su recibo, de forma que se pueda dar cumplimiento a la obligación de incluir la leyenda que diga “reclamo en trámite” y la naturaleza del mismo dentro del registro individual, lo cual deberá hacer el operador dentro de los dos (2) días hábiles siguientes a haber recibido la información de la fuente.

5. Para dar respuesta a la petición o reclamo, el operador o la fuente, según sea el caso, deberá realizar una verificación completa de las observaciones o planteamientos del titular, asegurándose de revisar toda la información pertinente para poder dar una respuesta completa al titular.

6. Sin perjuicio del ejercicio de la acción de tutela para amparar el derecho fundamental del hábeas data, en caso que el titular no se encuentre satisfecho con la respuesta a la petición, podrá recurrir al proceso judicial correspondiente dentro de los términos legales pertinentes para debatir lo relacionado con la obligación reportada como incumplida. La demanda deberá ser interpuesta contra la fuente de la información la cual, una vez notificada de la misma, procederá a informar al operador dentro de los dos (2) días hábiles siguientes, de forma que se pueda dar cumplimiento a la obligación de incluir la leyenda que diga “información en discusión judicial” y la naturaleza de la misma dentro del registro individual, lo cual deberá hacer el operador dentro de los dos (2) días hábiles siguientes a haber recibido la información de la fuente y por todo el tiempo que tome obtener un fallo en firme. Igual procedimiento deberá seguirse en caso que la fuente inicie un proceso judicial contra el titular de la información, referente a la obligación reportada como incumplida, y este proponga excepciones de mérito”.

Para el cumplimiento y control de lo que en esta normatividad se estipuló fue designada la Superintendencia de Industria y Comercio ejercerá que la función de vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, en cuanto se refiere a la actividad de administración de datos personales que se regula en la presente ley.

4.8 Ley 1273 de 2009

La norma enunciada establece nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las

empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

Acerca de esta nueva ley su coautor el intelectual Alexander Díaz García comenta:

> No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según la Revista Cara y Sello, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos[15].

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

El capítulo primero adiciona el siguiente articulado (subrayado fuera del texto):

[15] Ibid. DIAZ GARCÍA, Alexander.

Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Gracias a la tipificación de esta conducta, cada vez más frecuente, se salvaguarda la integridad física y lógica de las computadoras de personas del común y de entidades públicas y privadas, haciendo de un delito la conducta de inescrupulosos que a diario infectaban de manera indiscriminada a miles de usuarios de los servicios informáticos en todo el país castigando con severidad a quien produzca, trafique, adquiera, distribuya, venda, envíe, introduzca los denominados virus informáticos.

Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Al respecto es importante aclarar que la Ley 1266 de 2008 definió el término dato personal como “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica”. Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la ley obliga a quien “sustraiga” e “intercepte” dichos datos a pedir autorización al titular de los mismos.

Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos

legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Es primordial mencionar que este artículo tipifica lo que comúnmente se denomina “phishing”, modalidad de estafa que usualmente utiliza como medio el correo electrónico pero que cada vez con más frecuencia utilizan otros medios de propagación como por ejemplo la mensajería instantánea o las redes sociales. Según la Unidad de Delitos Informáticos de la Policía Judicial (Dijín) con esta modalidad se robaron más de 3.500 millones de pesos de usuarios del sistema financiero en el 2006

Un punto importante a considerar es que el artículo 269H agrega como

circunstancias de agravación punitiva de los tipos penales descritos anteriormente el aumento de la pena de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para si o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Es de anotar que estos tipos penales obligan tanto a entidades públicas o

privadas, como a personas naturales a prestar especial atención al tratamiento de equipos informáticos así como al tratamiento de los datos personales más teniendo en cuenta la circunstancia de agravación del inciso 3 del artículo 269H que señala “por quien tuviere un vínculo contractual con el poseedor de la información”.

Por lo tanto, se hace necesario tener unas condiciones de contratación, tanto con empleados como con contratistas, claras y precisas para evitar incurrir en la tipificación penal.

Por su parte, el capítulo segundo establece:

Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal.

La anterior descripción normativa hace referencia a que la persona que realice hurto superando las medidas de seguridad informáticas, manipulando un sistema informático, una red de sistema electrónico u otro medio semejante incurrirá en prisión de tres (3) a ocho (8) años. Un ejemplo de esta típica

conducta es evidenciado cuando se cometen hurtos a cajeros automáticos, dado que reúnen todos los elementos que constituyen este tipo de delitos.

Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

De esta manera, la Ley 1273 agrega como circunstancia de mayor punibilidad en el artículo 58 del Código Penal el hecho de realizar las conductas punibles utilizando medios informáticos, electrónicos ó telemáticos.

Como se puede apreciar, la Ley 1273 es un paso importante en la lucha contra los delitos informáticos en Colombia, por lo que es necesario que se esté preparado legalmente para enfrentar los retos que plantea.

En este sentido y desde un punto de vista empresarial, la nueva ley pone de presente la necesidad para los empleadores de crear mecanismos idóneos para la protección de uno de sus activos más valiosos como lo es la información.

Las empresas deben aprovechar la expedición de esta ley para adecuar sus contratos de trabajo, establecer deberes y sanciones a los trabajadores en los reglamentos internos de trabajo, celebrar acuerdos de confidencialidad con los mismos y crear puestos de trabajo encargados de velar por la seguridad de la información.

Por otra parte, es necesario regular aspectos de las nuevas modalidades laborales tales como el teletrabajo o los trabajos desde la residencia de los trabajadores los cuales exigen un nivel más alto de supervisión al manejo de la información.

De este modo, resulta conveniente dictar foros y seminarios al interior de las organizaciones con el fin de que los trabajadores sean consientes del nuevo rol que les corresponde en el nuevo mundo de la informática.

Lo anterior, teniendo en cuenta los perjuicios patrimoniales a los que se pueden enfrentar los empleadores debido al uso inadecuado de la información por parte de sus trabajadores y demás contratistas.

Pero más allá de ese importante factor, con la promulgación de esta ley se obtiene una herramienta importante para denunciar los hechos delictivos a los que se pueda ver afectado, un cambio importante si se tiene en cuenta que anteriormente las empresas no denunciaban dichos hechos no sólo para evitar daños en su reputación sino por no tener herramientas especiales.

CONCLUSIÓN

En el arduo proceso investigativo que conllevó la elaboración de este trabajo, se observaron varias conclusiones que se deben connotar para garantizar que se cumplió con el propósito que acarrea una investigación, en este orden de ideas debemos entonces dar inicialmente respuesta a la interrogante que dio origen a este compromiso.

¿Cuál es el Papel del Derecho Penal Moderno en su lucha contra el Delito Informático?

El derecho penal colombiano se enfrentó a uno de sus mayores retos como lo eran los delitos informáticos, los cuales eran conductas complejas por cuanto descubrir al autor de dichos delitos era prácticamente imposible debido a su pericia en el área de la informática y la negligencia del aparato judicial que no contaba con los recursos humanos y financieros para la capacitación de los funcionarios en la lucha contra este nuevo flagelo, que venía a convertirse en una amenaza inminente.

Sin embargo el legislador ante la problemática social suscitada por esta nueva forma de delito instituyó la herramienta jurídica idónea, de la cual Colombia está plenamente satisfecha, ello fue la ley 1273 de 2009, norma encaminada a

modernizar la legislación penal colombiana y a ponerla a la par de la de los países más desarrollados del mundo, como lo son los que integran la comunidad económica europea, que se viene desarrollando, a partir de acuerdos internacionales tan importantes como el Convenio sobre Cibercriminalidad suscrito en Budapest por los Estados Miembros del Consejo de Europa y por otros Estados firmantes, el 23 de noviembre de 2001, que entró en vigor desde el primero de julio de 2004 y que ha sido ratificada por una veintena de países debido a que busca impulsar una política penal común destinada a prevenir la criminalidad en el ciberespacio y, sobre todo, hacerlo mediante la adopción de una legislación apropiada de cara a la mejora de la cooperación internacional en tan delicadas e importantes materia.

Si bien, por razones obvias, Colombia no forma parte de ese organismo ni tampoco ha firmado el susodicho Convenio, era de vital importancia que la normatividad expedida recogiera esas directrices que son, además, las que las legislaciones europeas y de otros continentes empiezan a introducir en los respectivos ordenamientos jurídicos.

Por consiguiente, los Ponentes consideran que esta ley se ajusta a las necesidades sociales y jurídico-penales, cuales eran las de dotar a ordenamiento jurídico y a los organismos judiciales de un instrumento adecuado para proteger el bien jurídico de la información, en virtud del cual sea posible

enfrentar los graves riesgos que en estos tiempos padecen las redes informáticas y la información electrónica, que vienen siendo utilizadas para cometer graves infracciones penales. A razón de lo anteriormente expuesto se puede decir con toda seguridad que el derecho penal colombiano se encuentra totalmente preparado y actualizado para la larga lucha en contra de los delitos informáticos.

Hay que tener en consideración que para ganar la disputa contra este flagelo el Estado colombiano debe invertir mucho más recursos en el fortalecimiento del aparato judicial, esto conlleva a capacitación de sus fiscales, investigadores, policía judicial y auxiliares de la justicia, en la confrontación de este tipo de delitos así como también dotar a la fuerza pública de la tecnología necesaria para lograr este cometido en todo el país.

Engranando la realidad jurídica colombiana con un aparato judicial moderno y capacitado Colombia logrará su objetivo fundamental que es disminuir los delitos informáticos y acabar con la impunidad en este tipo de conductas.

Otra de las conclusiones hace referencia al fenómeno del ciberterrorismo, que es y será una amenaza real para la población mundial y se intensifica a medida que una nación desarrolla o adopta nuevas tecnologías e implementa éstas con apoyo en las redes públicas de información. Por ello, antes que se produzcan

resultados realmente catastróficos, es preciso comenzar a plantear soluciones definitivas al problema en el campo del derecho, para buscar una respuesta adecuada a las nuevas amenazas, sin sacrificar los recientes contenidos de los derechos que se crearon a los usuarios de las redes públicas de información.

RECOMENDACIONES

En Colombia es aconsejable que se establezca, mediante una ley, la regulación de la responsabilidad de los proveedores de servicios de Internet asimilando de manera critica la experiencia internacional pues hasta ahora además de las reglas tradicionales solo existe la propuesta de regulación por la vía del tratado de libre comercio con los Estados Unidos.

También es necesario que se fortalezcan las políticas públicas con respecto a la formación, enseñanza y capacitación de las comunidades acerca del manejo de la grandes redes de información debido a que ningún programa ni aplicación, en la era cibernética, es ciento por ciento seguro, de modo que los usuarios de las redes pueden acceder a ellos sin necesidad de mayores desarrollos. Este hecho impone la necesidad de diversificar el avance informático para mantener abierta la red pública a todos los usuarios del mundo, y desarrollar una red privada en aquellos aspectos en los que el acceso a los programas y aplicaciones y su manipulación malintencionada, pueda generar graves riesgos a la comunidad.

Asimismo el sector financiero debe aumentar y diversificar sus políticas de seguridad de la mano con las autoridades públicas, con la finalidad educar a los usuarios de estas entidades acerca del cuidado que corresponde utilizar los

diferentes servicios financieros a través de la red, disminuyendo ostensiblemente la capacidad de daño que pueden generar los delincuentes informáticos.

De la misma manera se hace imperiosa la necesidad de adoptar políticas claras y concretas en las universidades, centros académicos, fundaciones académicas y corporaciones educativas, acerca del debido uso del internet y de la información, con el fin de fomentar una cultura de prevención y manejo adecuado en los estudiantes, sin tener en cuenta si son de entidades de origen público o privado ya que es una problemática social que afecta a todos los rincones de la comunidad.

De igual forma esta cultura de prevención y manejo adecuado hacia el internet y la información debe ser transmitida en todas las aulas de clases de todas las instituciones educativas del territorio colombiano. Si todos los sectores de la sociedad trabajan en este objetivo común el delito informático dejara de ser un problema social y pasará a ser simplemente un obstáculo superado por la sociedad.

BIBLIOGRAFÍA

DÍAZ GARCÍA, Alexander. Derecho informático. Elementos de la Informática Jurídica. Editorial Leyer, Bogotá 2007. Pag.208

GIRALDO ANGEL, Jaime. Informática jurídica documental, Temis, Colombia. 1999. Pag.192

HORTE MARTÍNEZ, Raymond, Ciberterrorismo, ALFA-REDI, Revista de derecho informático, Edición electrónica, N° 082-Mayo, 2005. Pag.36

RIVERA LLANO, Abelardo, Dimensiones de la informática en el derecho (perspectivas y problemas), Ediciones Jurídica radar, Bogotá, 1999. Pag.285

TÉLLEZ VALDÉS, Julio. Derecho informático, Publicado por McGraw Hill, 1996. Pag.445

UNIVERSIDAD EXTERNADO DE COLOMBIA, Derecho Penal y Criminología. Volumen XXVIII -Numero 84-MAYO-AGOSTO de 2007. Pag.125

AYUDAS BIBLIOGRÁFICAS

Constitución Política de Colombia.

Ley 527 de 1999

Ley 599 de 2000

Ley 603 de 2000

Ley 679 de 2001

Ley 1266 de 2008

Ley 1273 de 2009

Corte Constitucional Sentencia C- 662 de 8 de junio de 2000

Corte Suprema de Justicia. Sala de Casación Penal. Sentencia del 30 de Abril de 2008 (Proceso No. 29188)

www.washintonpost.com/wp-dyn/contesf/article

www.astrolabio.net/datafiles/1160518424.html

WIKIPEDIA, La enciclopedia libre, Internet.

www.delitosinformaticos.com/delitos/colombia

www.derechoinformatico.uchile.

www.sabanet.unisabana.edu.co/derecho/semestre2/telematica/software/delitosinformaticos.ppt.